Symantec AntiVirus™ Corporate Edition Installation Guide

Symantec AntiVirus™ Corporate Edition Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version 10.0
PN: 10362883

Copyright Notice

Copyright © 2005 Symantec Corporation.
All Rights Reserved.
Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.
NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.
No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, LiveUpdate, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Norton Internet Security, Norton Personal Firewall, Symantec AntiVirus, Symantec Client Firewall, Symantec Client Security, and Symantec Security Response are trademarks of Symantec Corporation.
Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
Symantec AntiVirus

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the total number of copies You may use, in any combination of Software titles, may not exceed the total number of copies indicated in the License Module. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. use the Software in accordance with any written agreement between You and Symantec; and
E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antispam software utilize updated antispam rules; antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; policy compliance software utilize updated policy compliance updates; and vulnerability assessment products utilize updated vulnerability signatures; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring

purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of thirty (30) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

A. If the Software You have licensed is a specified Symantec AntiVirus for a corresponding third party product or platform, You may only use that specified Software with the corresponding product or platform. You may not allow any computer to access the Software other than a computer using the specified product or platform. In the event that You wish to use the Software with a certain product or platform for which there is no specified Software, You may use Symantec AntiVirus Scan Engine.
B. If the Software you have licensed is Symantec AntiVirus utilizing Web Server optional licensing as set forth in the License Module, the following additional use(s) and restriction(s) apply:
i) You may use the Software only with files that are received from third parties through a web server;
ii) You may use the Software only with files received from less than 10,000 unique third parties per month; and
iii) You may not charge or assess a fee for use of the Software for Your internal business.
C. If the Software You have licensed is Symantec Client Security, this Software utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright (c) 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright (c) 1994. Hewlett-Packard Company.

Sun Microsystems, Inc. Binary Code License Agreement

READ THE TERMS OF THIS AGREEMENT AND ANY PROVIDED SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT") CAREFULLY BEFORE OPENING THE SOFTWARE MEDIA PACKAGE. BY OPENING THE SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THESE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF THE SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT.

1. LICENSE TO USE.

Sun grants you a non-exclusive and non-transferable license for the internal use only of the accompanying software and documentation and any error corrections provided by Sun (collectively "Software"), by the number of users and the class of computer hardware for which the corresponding fee has been paid.

2. RESTRICTIONS.

Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Except as specifically authorized in any Supplemental License Terms, you may not make copies of Software, other than a single copy of Software for archival purposes. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. Licensee acknowledges that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement.

3. LIMITED WARRANTY.

Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software.

4. DISCLAIMER OF WARRANTY.

UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

5. LIMITATION OF LIABILITY.

LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose.

6. Termination.

This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Upon Termination, you must destroy all copies of Software.

7. Export Regulations.

All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

8. U.S. Government Restricted Rights.

If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and

with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

9. Governing Law.

Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

10. Severability.

If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

11. Integration.

This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

JAVA™ 2 RUNTIME ENVIRONMENT (J2RE), STANDARD EDITION, VERSION 1.4.2_X SUPPLEMENTAL LICENSE TERMS

These supplemental license terms ("Supplemental Terms") add to or modify the terms of the Binary Code License Agreement (collectively, the "Agreement"). Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

1. Software Internal Use and Development License Grant.

Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the binary form of the Software complete and unmodified for the sole purpose of designing, developing, testing, and running your Java applets and applications intended to run on Java-enabled general purpose desktop computers and servers ("Programs").

2. License to Distribute Software.

Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. (vi) include the following statement as part of product documentation (whether hard copy or electronic), as a part of a copyright page or proprietary rights notice page, in an "About" box or in any other form reasonably designed to make the statement visible to users of the Software: "This product includes code licensed from RSA Security, Inc.", and (vii) include the statement, "Some portions licensed from IBM are available at http://oss.software.ibm.com/icu4j/".

3. License to Distribute Redistributables.

Subject to the terms and conditions of this Agreement, including but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (v) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software, (vi) include the following statement as part of product documentation (whether hard copy or electronic), as a part of a copyright page or proprietary rights notice page, in an "About" box or in any other form reasonably designed to make the statement visible to users of the Software: "This product includes code licensed from RSA Security, Inc.", and (vii) include the statement, "Some portions licensed from IBM are available at http://oss.software.ibm.com/icu4j/".

4. Java Technology Restrictions.

You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of the "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional classes, interfaces, or

subpackages that are in any way identified as “java”, “javax”, “sun” or similar convention as specified by Sun in any naming convention designation.

5. Notice of Automatic Software Updates from Sun.

You acknowledge that the Software may automatically download, install, and execute applets, applications, software extensions, and updated versions of the Software from Sun (“Software Updates”), which may require you to accept updated terms and conditions for installation. If additional terms and conditions are not presented on installation, the Software Updates will be considered part of the Software and subject to the terms and conditions of the Agreement.

6. Notice of Automatic Downloads.

You acknowledge that, by your use of the Software and/or by requesting services that require use of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun (“Other Software”). Sun makes no representations of a relationship of any kind to licensors of Other Software. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Trademarks and Logos.

You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations (“Sun Marks”), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun’s benefit.

8. Source Code.

Software may contain source code that is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

9. Termination for Infringement.

Either party may terminate this Agreement immediately should any Software become, or in either party’s opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.
(LFI#124423/Form ID#011801)

Contents

Technical support

Chapter 1 Introducing Symantec AntiVirus

About Symantec AntiVirus 19
What's new in this release 20
Components of Symantec AntiVirus 22
How Symantec AntiVirus works 24
What you can do with Symantec AntiVirus 25
Where to get more information about Symantec AntiVirus 26

Chapter 2 Planning the installation

Plan your network architecture 29
Administrative rights and .msi files 33
About setting administrative rights to target computers 33
About customizing installations by using .msi options 34
About configuring user rights with Active Directory 34
System time requirements 34
System requirements 34
Required protocols 35
Operating system requirements 36
RAM, storage, and application requirements 37
Disabling Windows XP firewalls 39
Disabling Internet Connection Firewall 39
Disabling Windows Firewall 39
About using Windows XP firewalls 40
Permitting remote software installation on Windows XP computers 40
About disabling other anti-security-risks programs 41

Chapter 3 Installing Symantec AntiVirus for the first time

Before you install 43
About client installation 44
Installation sequence 44
Symantec System Center installation on server operating systems 44
Installing the Symantec System Center 45

Installing a management server from the Symantec System Center 50
Configuring your server group 54
Configuring a primary management server 54
Protecting your server group root certificate private key 56
Configuring updates and protection 57
Installing client software 60
About disabling the Windows XP firewall 60
Installing client software by using the Symantec System Center 60
Installing client software from the CD 62
Testing antivirus capabilities 63
Testing antivirus configuration 64
Testing Auto-Protect 64
Testing Threat Tracer 65

Chapter 4 Migrating to the current version of Symantec AntiVirus

About migration 67
About migrating to the SSL communications architecture 68
Disable security risk programs from other vendors 70
How migration works 70
Steps to migrating to the current version 71
Supported and unsupported server and client migration paths 72
Supported migration paths 72
Unsupported migration paths 73
Unsupported migration of Administrator tools 73
Custom settings may be lost 73
Quarantine items are automatically migrated 74
Symantec System Center upgrade scenarios 74
Upgrading the Symantec System Center 76
Before you upgrade the Symantec System Center 76
Upgrading the Symantec System Center for your scenario 77
Installing the Symantec System Center 79
Unlocking the migrated server group 79
Migrating management servers 80
Before you migrate management servers 81
Migrating the first management servers 81
About migrating subsequent servers 82
Migrating from Symantec AntiVirus on NetWare platforms 83
Preventing errors when the logon script is used 84
About VPStart commands 84
About migration from other server antivirus products 85

Migrating client software 85
Before you migrate client software 85
Migrating clients by using the CD 86
Migrating clients by using the Symantec System Center 86
Additional client migration methods 86
How to determine parent servers and policy 87
Other antivirus product client migrations 87
About migrating LiveUpdate servers 87

Chapter 5 Installing Symantec AntiVirus management components

Before you install 89
How to prepare for the Symantec System Center installation 90
Symantec System Center installation and Terminal Services 90
Symantec System Center installation 91
Installing and configuring the Central Quarantine 91
Installing the Quarantine Console snap-in 92
Installing the Quarantine Server 93
Attaching a management server to the Central Quarantine 98
Configuring servers and clients to use the Central Quarantine 98
Installing and configuring the LiveUpdate Administration Utility 99
Uninstalling Symantec AntiVirus management components 102
Uninstalling the Symantec System Center 102

Chapter 6 Installing Symantec AntiVirus servers

Before you install 103
TCP and legacy UDP communications 104
Management servers and certificates 105
Server installation methods 105
Why AMS^2 is installed with Symantec AntiVirus server 106
About customizing server installations by using .msi options 107
About configuring user rights with Active Directory 107
Preparations for Symantec AntiVirus server installation 107
Installing Symantec AntiVirus servers locally 113
Deploying the server installation across a network connection 115
Starting the server installation 116
Running the server setup program 117
Selecting computers to which you want to install 119
Completing the server installation 122
Checking for errors 126
Manually loading the Symantec AntiVirus NLMs 126
Installing with NetWare Secure Console enabled 127
Installing with the server installation package 128

About installing servers by using Microsoft SMS 129
Manually installing AMS^2 server 130
Uninstalling Symantec AntiVirus server 130

Chapter 7 Installing Symantec AntiVirus clients

Before you install 134
About creating a primary management server 134
About client installation methods 135
About customizing client installation files by using .msi options 136
About configuring user rights with Active Directory 136
About Symantec AntiVirus client on a Terminal Server 136
About Windows cluster server protection 137
About email support 137
About the client configurations file 139
Installing Symantec AntiVirus clients locally 139
Deploying the client installation across a network connection 143
Starting the client installation 143
Running the client setup program 144
Installing from the client installation folder on the server 147
Web-based deployment 148
Web-based deployment requirements 148
About the Web server installation 149
Setting up the Web server 149
Customizing the deployment files 152
Testing the installation 154
How to notify users of the download location 154
Installing clients by using logon scripts 155
Configuring automatic client installations from NetWare servers 157
About installing clients using third-party products 158
About installing clients with Active Directory and Tivoli 158
About installing clients with Microsoft SMS 158
About installing clients with Novell ZENworks 159
Post-installation client tasks 160
Configuring clients with the Grc.dat configuration file 160
Copying the configuration files from a management server 160
Pasting the configuration files on the client 161
Uninstalling Symantec AntiVirus clients 161

Appendix A Windows Installer (.msi) command-line reference

Installing Symantec AntiVirus using command-line parameters 163
Default Symantec AntiVirus server installation 164
Default Symantec AntiVirus client installation 164

Windows Installer commands 165
Server installation properties and features 167
Symantec AntiVirus server properties 167
Symantec AntiVirus server features 168
Client installation properties and features 169
Symantec AntiVirus client properties 169
Windows Security Center features 170
Symantec AntiVirus features 171
Symantec AntiVirus client features 171
Using the log file to check for errors 172
Identifying the point of failure of an installation 173
Command-line examples 173

Index

Chapter 1

Introducing Symantec AntiVirus

This chapter includes the following topics:

- About Symantec AntiVirus
- What's new in this release
- Components of Symantec AntiVirus
- How Symantec AntiVirus works
- What you can do with Symantec AntiVirus
- Where to get more information about Symantec AntiVirus

About Symantec AntiVirus

Symantec AntiVirus Corporate Edition (Symantec AntiVirus) provides scalable, cross-platform antivirus protection for workstations and network servers throughout the enterprise. By using the enhanced security features and centralized policy management of Symantec AntiVirus, administrators can manage clients and servers that are assigned to logical groups. In addition, administrators can create, deploy, and lock down security policies and settings to keep systems up-to-date and properly configured at all times. The central management console enables administrators to audit the network, identify unprotected nodes, and apply the appropriate security protection before a threat occurs.

What's new in this release

Symantec AntiVirus includes new features, as well as improvements to existing features.

Table 1-1 lists and describes what's new in this release.

Table 1-1 New features in Symantec AntiVirus

Feature	Description
Security risk detection and removal	Auto-Protect and all other scans now detect security risks such as spyware and adware in addition to viruses. Upon detection, security risks and viruses are removed, and the modifications that security risks and viruses make to computers are reverted. Auto-Protect works with Quick Scan, which primarily scans common registry keys for references to unwanted malicious files. Auto-Protect also lets you specify exclusions.
Roles-based administrative accounts at the server group level	Lets you set up roles-based user accounts in the Symantec System Center™. The following roles are available: ■ Read-only ■ Administrator ■ Central Quarantine ■ Gateway Security
SSL communications and digital certificates	SSL secures communications between management consoles, servers, and clients. Digital certificates are used to authenticate users and servers before they are allowed to implement configuration changes. With Symantec AntiVirus, you now have the following assurances: ■ Only authorized users can issue configuration commands. ■ Data is transmitted and received between intended entities only. ■ Data that is transmitted and received between intended entities is not tampered with or modified. ■ Data that is transmitted and received between intended entities is not revealed to unauthorized entities.
Tamper Protection	Automatically protects Symantec product processes, from being tampered with by unauthorized processes and users. Also lets you specify exclusions.

Table 1-1 New features in Symantec AntiVirus

Feature	Description
Windows Security Center and Windows Firewall configuration	Lets you disable Windows Security Center for Windows® XP with Service Pack 2, and configure antivirus definition alerts. Lets you disable Windows Firewall for Windows Security Center and suppress any messages about the Windows Firewall that are directed to users.
Server Tuning Options	Lets you tune client tracking options from the Symantec System Center, such as client check-in times, the number of clients to process before pausing, and the pause time interval. Also lets you enable support for legacy servers and clients, and tune how virus definitions updates are distributed, such as setting the number of threads to use, time intervals, and so on.
Threat Detection in alternate data streams	Scans now search for viruses and threats in alternate data streams.
AMD 64-bit support	Symantec AntiVirus now supports AMD® 64-bit Opteron™ and Athlon™ processors as an antivirus client.
Quick Scan	Quickly scans for the most common viruses and security risks that might be loaded into memory and in common infection locations.
Full Scan	Thoroughly scans for all viruses and security risks in the boot sector, registry, programs that are loaded into memory, and all files and folders.
Dropped support for IPX protocol	Symantec AntiVirus management communications no longer supports the IPX protocol.
Dropped support for 7.6 client management	This version of Symantec AntiVirus no longer supports the management of version 7.6 clients, but does support the migration of the clients to this version.

Components of Symantec AntiVirus

Table 1-2 lists and describes the main components of Symantec AntiVirus.

Table 1-2 Components of Symantec AntiVirus

Component	Description
The Symantec System Center	Performs management operations such as the following: ■ Installing antivirus protection on workstations and network servers. ■ Updating virus definitions. ■ Managing network servers and workstations running Symantec AntiVirus.
Symantec AntiVirus server	■ Protects the supported Windows® and NetWare® computers. ■ Pushes configuration and virus definitions files updates to managed clients.
Symantec AntiVirus client	Provides antivirus protection for networked and non-networked computers. Symantec AntiVirus protects supported Windows computers.
LiveUpdate™	Provides the capability for computers to automatically pull updates of virus definitions files from the Symantec LiveUpdate server or an internal LiveUpdate server.
Central Quarantine	Works as part of the Digital Immune System™ to provide automated responses to heuristically detected new or unrecognized viruses and does the following: ■ Receives unrepaired infected items from Symantec AntiVirus servers and clients. ■ Forwards suspicious files to Symantec™ Security Response. ■ Returns updated virus definitions to the submitting computer.

Table 1-3 lists and describes the Symantec System Center management components, which are installed by default.

Table 1-3 Symantec System Center management components

Component	Description	Overview
The Symantec System Center console	The Symantec System Center is the console that you use to administer managed Symantec products. The Symantec System Center is a stand-alone application that runs under Microsoft® Management Console.	■ Install the Symantec System Center console to the computers from which you plan to manage Symantec AntiVirus. ■ Install to at least one computer to view and administer your network. If your organization is large or you work out of several offices, you can install the Symantec System Center to as many computers as you need. Rerun the installation program and select the appropriate option. ■ The Symantec System Center does not need to be installed on a network server or an antivirus server.
Alert Management System^2 (AMS^2) console	The AMS^2 console provides alerts from AMS^2 clients and servers. When you install the AMS^2 console, you can configure alert actions for Symantec AntiVirus servers that have the AMS^2 service installed. When a problem occurs, AMS^2 can send alerts through a pager, an email message, and other means.	■ Install the AMS^2 console to the same computer on which the Symantec System Center console is installed. ■ Install the AMS^2 service to one or more primary servers on which Symantec AntiVirus server is installed. ■ If you choose not to install AMS^2, you can use the notification and logging mechanisms that are available from the Symantec System Center. ■ If you plan to implement Symantec Enterprise Security alerting instead of AMS^2, you do not need to install AMS^2.

Table 1-3 Symantec System Center management components

Component	Description	Overview
Symantec AntiVirus snap-in	This management snap-in for the Symantec System Center lets you manage Symantec AntiVirus on workstations and network servers.	Install this component to do the following from the Symantec System Center: ■ Set up and administer Symantec AntiVirus server and client groups. ■ Manage antivirus protection on computers that run Symantec AntiVirus. ■ Configure groups of computers that run Symantec AntiVirus. ■ Manage events. ■ Configure alerts. ■ Perform remote operations, such as virus scans and virus definitions files updates.
ClientRemote Install tool	This tool lets you remotely install Symantec AntiVirus to one or more Windows-based computers. You can also run this tool from the Symantec AntiVirus CD.	Install this component to manage remote client installations.
AV Server Rollout tool	This tool lets you remotely install Symantec AntiVirus server to the Windows-based computers and NetWare servers that you select. You can also run this tool from the Symantec AntiVirus CD.	Install this component to manage remote server installations from the Symantec System Center.

How Symantec AntiVirus works

Symantec AntiVirus lets you deploy and centrally manage virus definitions files and firewall policy files on clients according to the requirements of your enterprise. To protect against viruses and other threats that are not yet defined in files, you can use the Digital Immune System.

The Digital Immune System is a fully automated, closed-loop antivirus system that manages the entire antivirus process, including virus discovery, virus analysis, and the deployment and repair of files that could not be repaired on a client computer. This automated system dramatically reduces the time between when a virus is found and when a repair is deployed, which decreases the severity of many threats.

The Digital Immune System works with the Central Quarantine and performs the following actions:

- Identifies and isolates viruses
  When a client computer that is configured to repair infected files cannot repair a specific file, it forwards the file first to the local Quarantine, and then to the Central Quarantine Server where more current virus definitions might be available.
- Rescans the file and submits viruses to Symantec™ Security Response
  If the Central Quarantine has more current virus definitions than the submitting computer, it might be able to fix the file. If so, it pushes the newer definitions to the submitting computer. If the file cannot be repaired, it is sent to a Symantec Security Response gateway for further analysis.
- Analyzes submissions, and generates and tests repairs
  When the Digital Immune System receives a new submission, it analyzes the virus, generates the repair, and tests it. Then it builds new virus definitions files, including the new virus fingerprint, and returns the new virus definitions files to the gateway. Usually, this process occurs automatically; however, some cases require Symantec Security Response to intervene.
- Deploys repairs
  The Quarantine Agent downloads the new virus definitions and installs them on the Central Quarantine Server. The updated definitions are then pushed to the submitting computer, if they are needed.

For details about configuring the Central Quarantine and about using the Digital Immune System, see the *Symantec Central Quarantine Administrator's Guide*.

What you can do with Symantec AntiVirus

Symantec AntiVirus lets you do the following:

- Protect against viruses, blended threats, and security risks such as adware spyware.
- Manage the deployment, configuration, updating, and reporting of antivirus protection from an integrated management console
- Manage Symantec AntiVirus clients based on their connectivity.
- Quickly respond to virus outbreaks and deploy updated virus definitions.

- Provide a high level of protection and an integrated response to security threats for all users that connect to your network, including telecommuters with connections that are always on, and mobile users with intermittent connections to your network.
- Obtain a consolidated view of multiple security components across all of the workstations on your network.
- Perform a customizable, integrated installation of all of the security components and set policies simultaneously.
- Establish and enforce security policies.
- View histories and log data.

Where to get more information about Symantec AntiVirus

Sources of information on using Symantec AntiVirus include the following:

- *Symantec AntiVirus Administrator's Guide*
- *Symantec AntiVirus Reference Guide*
- *Symantec AntiVirus Client Guide*
- *LiveUpdate Administrator's Guide*
- *Symantec Central Quarantine Administrator's Guide*
- Online Help that contains all of the content that is found in the above guides and more

The primary documentation is available in the Docs folder on the Symantec AntiVirus CD. Some individual component folders contain component-specific documentation. Updates to the documentation are available from the Symantec Technical Support and Platinum Support Web sites.

Additional information is available from the Symantec Web sites listed in Table 1-4.

Table 1-4 Symantec Web sites

Types of information	Web address
Public Knowledge Base Releases and updates Manuals and documentation Contact options	http://www.symantec.com/techsupp/enterprise/
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Platinum Support Web access	https://www-secure.symantec.com/platinum/

Chapter 2

Planning the installation

This chapter includes the following topics:

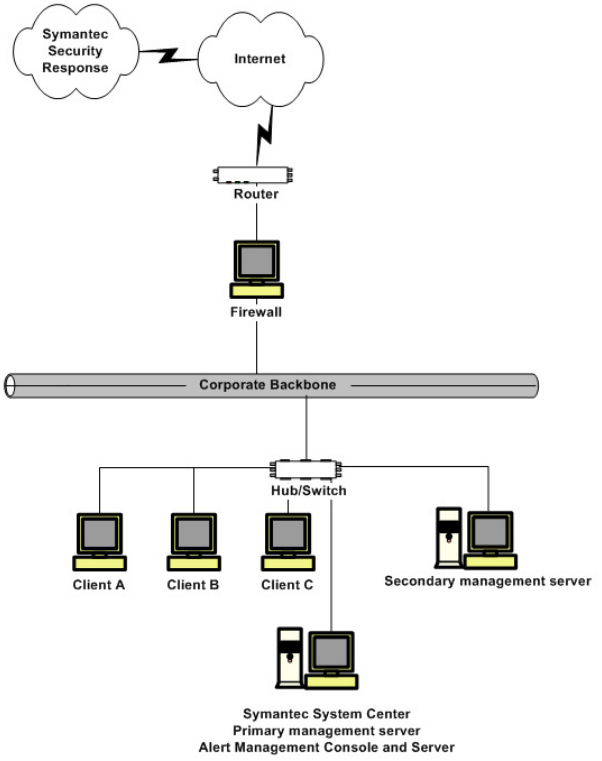
- Plan your network architecture
- Administrative rights and .msi files
- System time requirements
- System requirements
- Disabling Windows XP firewalls
- About using Windows XP firewalls
- Permitting remote software installation on Windows XP computers
- About disabling other anti-security-risks programs

Plan your network architecture

Symantec AntiVirus installation configurations scale from small to large deployments. In small deployments that support up to 100 clients, you can install all management components and servers on one computer.

Figure 2-1 illustrates how Symantec AntiVirus management and server software are collocated in a small deployment.

Figure 2-1 Small deployment



With this architecture, administrators use the Symantec System Center and a primary management server on one computer to manage and update clients with virus definitions files. Clients might be attached to hubs, which creates a flat network. Clients might be segmented with switches into different subnets, which is an efficient way to conserve bandwidth. You manage this architecture with one server group, which you create by using the Symantec System Center.

This architecture also illustrates a best practice of creating a secondary management server in a server group. When a server group contains two or more management servers, every server other than the primary management server is defined as a secondary management server. Symantec AntiVirus management servers do not require server operating systems, but do not support email scanning like the clients.

If your server group contains one management server only, which would be the primary, and if that server crashes, you cannot unlock and manage the server group from the Symantec System Center. If you have a secondary management

server in the group, you can unlock the server group. You can then migrate the clients that were managed by the crashed server to a new or existing server in the group by copying a Grc.dat file from the new or existing server to the clients.

See "Configuring clients with the Grc.dat configuration file" on page 160.

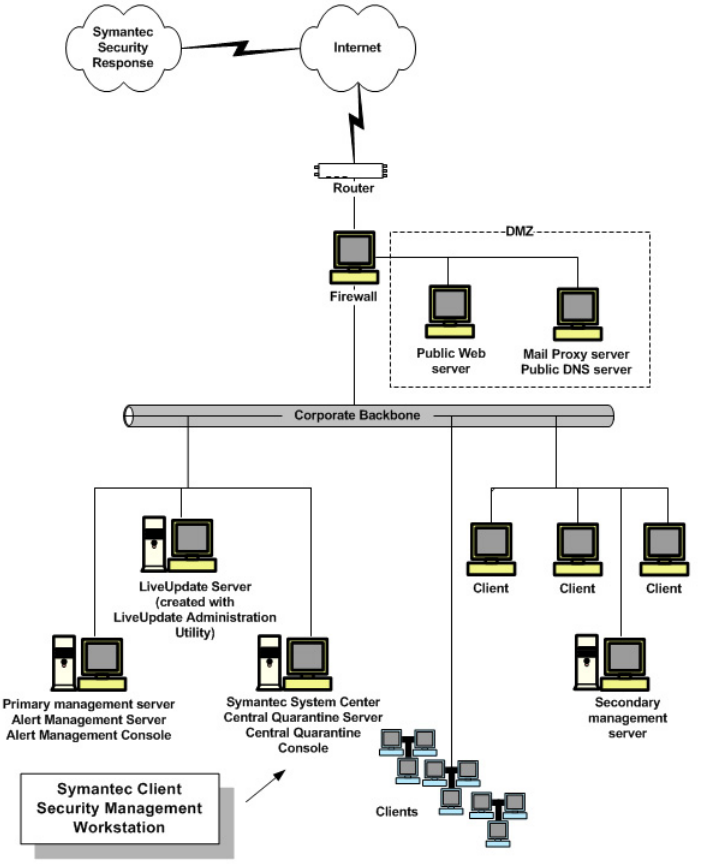
If you do not create a secondary management server in your server group, back up the pki directory and all subdirectories. If your primary server becomes corrupt, you can re-create it if you have the backup files to restore. For details, refer to the Knowledge Base articles on the Symantec Web site.

Note: For first-time installations, you should create and configure Symantec AntiVirus as shown in Figure 2-1, with one primary management computer that is dedicated to managing a few clients, and a secondary management server for disaster recovery purposes if the primary management server fails.

In large deployments that might support thousands of client computers, you can distribute Symantec AntiVirus across your enterprise. For example, you can install management components on different computers, install antivirus servers on multiple computers, and install a LiveUpdate server, which provides a single point for downloading antivirus definitions.

Figure 2-2 illustrates how Symantec AntiVirus management and server software is distributed in a relatively large deployment.

Figure 2-2 Large deployment



With this architecture, one computer runs the Symantec System Center, which lets administrators manage multiple server and client groups and a Central Quarantine server. This architecture also deploys a separate LiveUpdate server from which antivirus servers and clients receive the latest virus definitions files. By using a LiveUpdate server, only one computer retrieves the virus definitions files over the Internet, which preserves firewall bandwidth.

It is possible to manage over 100,000 clients with each antivirus management server, both primary and secondary, so it is possible to manage very large environments with one server group. Most large environments, however, configure server groups by geographic location, and might use one server group for email servers, which have special requirements. For details, refer to the *Symantec AntiVirus Reference Guide*.

In large deployments, you might also need to tune how virus definitions update files are distributed by specifying the number of threads to use on a server, and the time intervals to wait before pushing out additional updates. You can set these options by using the Server Tuning Options tabs in the Symantec System Center.

Note: Every server group, which you create and manage by using the Symantec System Center, requires one primary management server. As a best practice, each server group should contain at least one secondary management server for disaster recovery purposes. Very large deployments might use multiple instances of the Symantec System Center in different geographic locations. You should also archive the private key that is installed on the primary management server in the pki\private-keys directory as a best practice.

Administrative rights and .msi files

Review the information about administrative rights and .msi files to plan your installation.

About setting administrative rights to target computers

To install Symantec AntiVirus servers and clients to computers that run supported Windows operating systems, you must have administrator rights to the computer or to the Windows domain to which the computer belongs, and log on as administrator. The Symantec AntiVirus server installation program launches a second installation program on the computer to create and start services, and to modify the registry.

If you do not want to provide users with administrative rights to their own computers, use the ClientRemote Install tool in the Symantec System Center to remotely install Symantec AntiVirus clients to computers that run supported Windows operating systems. To run the ClientRemote Install tool, you must have local administrative rights to the computers to which you are installing the program.

See "Installing Symantec AntiVirus clients" on page 133.

About customizing installations by using .msi options

The Symantec AntiVirus client and server installation packages are Windows Installer (.msi) files that you can configure and deploy by using the standard Windows Installer options. You can use environment management tools that support .msi deployment, such as Active Directory® or Tivoli Enterprise Console®, to install clients on your network.

See "Windows Installer (.msi) command-line reference" on page 163.

About configuring user rights with Active Directory

If you are using Active Directory to manage Windows-based computers on your network, you can create a Group Policy that provides the necessary user rights to install Symantec AntiVirus.

For more information on using Active Directory, see the Active Directory documentation provided by Microsoft.

System time requirements

Symantec AntiVirus now uses the SSL protocol to transmit configuration information securely between management consoles, servers, and clients. Symantec AntiVirus also uses digital certificates to authenticate users and servers. To authenticate users, a login certificate is issued to them with a default time validity value of 24 hours.

Because the login certificate expires after a certain amount of time, the system clocks of all management console computers, servers, and clients must be within the default of 24 hours plus or minus of the system time on the primary management server. You can change this time by using the Symantec System Center. The login certificate is automatically reissued if it expires and the user account has not been revoked.

System requirements

Symantec AntiVirus requires specific protocols, operating systems and service packs, software, and hardware.

All of the requirements that are listed for Symantec AntiVirus components are designed to work with the hardware and software recommendations for the supported Windows and NetWare computers. All computers to which you are installing Symantec AntiVirus should meet or exceed the recommended system requirements for the operating system that is used.

Review the following requirements before you install Symantec AntiVirus:

- Required protocols
- Operating system requirements
- RAM, storage, and application requirements

Required protocols

Table 2-1 lists the communications requirements between the Symantec System Center and the various Symantec servers, consoles, and clients.

Table 2-1 Console and server to client communications

Protocol	Console and server ports	Client ports
TCP Communications	1024 - 4999 Console and server 2967 Console and server	2967 1024 - 5000
TCP Remote installation	1024 - 4999 Console 139 Server	139 1024 - 5000
UDP Discovery	38293 Server 1024 - 4999 Console	None

If your servers and clients run firewall software, and you want to manage these servers and clients, you must open these ports. Alternatively, permit Rtvscan.exe on all computers and Pds.exe on servers and consoles to send and receive traffic through your firewalls. Also, remote server and client installation tools require that TCP ports 139 and 1024 - 5000 be opened.

See "Disabling Windows XP firewalls" on page 39.

Note: If you are running Windows XP, system disk space usage will be increased if you have the System Restore functionality enabled. For more information on how System Restore works, see the Microsoft Operating System documentation.

Operating system requirements

Table 2-2 lists Symantec AntiVirus component operating system requirements.

Table 2-2 Operating system requirements

Component	Description
Symantec System Center	■ Windows® 2000 Professional/Server/Advanced Server ■ Windows XP Professional ■ Windows Server™ 2003 Web/Standard/Enterprise/ Datacenter
Symantec AntiVirus server	■ Windows 2000 Professional/Server/Advanced Server ■ Windows XP Professional ■ Windows Server 2003 Web/Standard/Enterprise/ Datacenter ■ NetWare 5.1 with Support Pack 8 or higher ■ NetWare 6.0 with Support Pack 5 or higher ■ NetWare 6.5 with Support Pack 2 or higher
Quarantine Console	■ Windows 2000 Professional/Server/Advanced Server ■ Windows XP Professional ■ Windows Server 2003 Web/Standard/Enterprise/ Datacenter
Central Quarantine Server	■ Windows 2000 Professional/Server/Advanced Server ■ Windows XP Professional
Symantec AntiVirus client 32-bit	■ Windows 2000 Professional/Server/Advanced Server ■ Windows XP Home Edition/Professional/Tablet PC Edition ■ Windows Server 2003 Web/Standard/Enterprise/ Datacenter
Symantec AntiVirus client 64-bit	■ Windows XP 64-bit Edition Version 2003 ■ Windows Server 2003 Enterprise/Datacenter 64-bit

RAM, storage, and application requirements

Pentium® II or higher processors are recommended for all 32-bit components.

Table 2-3 lists RAM, storage, and application requirements for Symantec AntiVirus components.

Table 2-3 RAM, storage, and application requirements

Component	RAM	Storage and Applications
Symantec System Center	64 MB	■ 36 MB disk space without snap-ins ■ 24 MB disk space for AMS^2 snap-in ■ 6 MB disk space for Symantec AntiVirus snap-in ■ 1 MB disk space for Symantec Client Firewall snap-in ■ 130 MB disk space for AV Server Rollout snap-in ■ 2 MB disk space for ClientRemote Install snap-in ■ Internet Explorer 5.5 with Service Pack 2 or later ■ Microsoft Management Console 1.2 or later If MMC is not already installed, you will need 3 MB free disk space (10 MB during installation). If version 1.2 or later is not on the computer to which you are installing, the installation program will install it.
Symantec AntiVirus server for Windows	64 MB	■ 140 MB disk space ■ 15 MB disk space for AMS^2 server files (if you choose to install the AMS^2 server) ■ Internet Explorer 5.5 with Service Pack 2 or later ■ Static IP address (recommended) **Note:** Symantec AntiVirus does not support the scanning of Macintosh® volumes on Windows servers for Macintosh viruses.
Symantec AntiVirus server for NetWare	15 MB	■ 116 MB disk space (70 MB disk space for server files and 46 MB disk space for the client disk image) ■ 20 MB disk space for AMS^2 server files (if you choose to install the AMS^2 server) ■ Static IP address (recommended) **Note:** Symantec AntiVirus is not supported on NetWare servers that run SFT III.

Table 2-3 RAM, storage, and application requirements

Component	RAM	Storage and Applications
Quarantine Console	64 MB	■ 35 MB disk space ■ Internet Explorer 5.5 Service Pack 2 or later ■ Microsoft Management Console version 1.2 or later If MMC is not already installed, you will need 3 MB free disk space (10 MB during installation).
Central Quarantine Server	128 MB	■ 40 MB disk space for Quarantine Server ■ 500 MB to 4 GB disk space recommended for quarantined items ■ Internet Explorer 5.5 with Service Pack 2 or later ■ Minimum swap file size of 250 MB **Note:** If you run Windows XP, system disk space usage is increased if the System Restore functionality is enabled. For more information on how System Restore works, see the Microsoft operating system documentation.
Symantec AntiVirus client 32-bit	64 MB	■ 55 MB disk space Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements: ■ Microsoft Terminal Server RDP (Remote Desktop Protocol) client ■ Citrix® Metaframe® (ICA) client 1.8 or later if using Citrix Metaframe server on Terminal Server
Symantec AntiVirus client 64-bit	80 MB	■ 70 MB disk space ■ Internet Explorer 5.5 with Service Pack 2 ■ Intel® processors that support Intel® Extended Memory 64 Technology (Intel® EM64T) ■ AMD 64-bit Opteron™ and Athlon™ processors

Note: The installation scripts do not check to verify that Internet Explorer 5.5 with Service Pack 2 or later is installed on computers when it is required. If the target computers do not have the correct version of Internet Explorer, the installation fails without informing you.

Disabling Windows XP firewalls

Windows XP and Windows 2003 Server contain firewalls that are enabled by default. If these firewalls are enabled, you might not be able to install server software or client software remotely from the Symantec System Center and other remote installation tools.

Disabling Internet Connection Firewall

Windows XP with Service Pack 1 includes a firewall called Internet Connection Firewall that can interfere with remote Symantec AntiVirus installation, and communications between servers and clients. If any of your servers or clients run Windows XP, you can disable the Windows XP firewall on them before you install Symantec AntiVirus clients.

To disable Internet Connection Firewall

1. On the Windows XP taskbar, click **Start > Control Panel**.
2. In the Control Panel window, double-click **Network Connections**.
3. In the Network Connections window, right-click the active connection, and then click **Properties**.
4. On the Advanced tab, under Internet Connection Firewall, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
5. Click **OK**.

Disabling Windows Firewall

Windows XP with Service Pack 2 and Windows 2003 Server include a firewall called Windows Firewall that can interfere with remote Symantec AntiVirus installation, and communications between servers and clients. If any of your servers or clients run Windows XP with Service Pack 2 or Windows Server 2003, you can disable the firewall on them before you install Symantec AntiVirus clients.

To disable Windows Firewall

1. On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel window, double-click **Network Connections**.
3. In the Network Connections window, right-click the active connection, and then click **Properties**.

4 On the Advanced tab, under Internet Connection Firewall, click **Settings**.

5 In the Windows Firewall window, on the General tab, uncheck **On (recommended)**.

6 Click **OK**.

About using Windows XP firewalls

To use the Windows XP firewalls, you need to configure them to support Symantec AntiVirus communications by opening ports or by specifying trusted programs. You can enable communications by permitting Rtvscan.exe on all computers and Pds.exe on servers and consoles to send and receive traffic through your firewalls.

Symantec AntiVirus clients use TCP ports 2967 and 1024-5000 for almost all communications with Symantec AntiVirus servers, so you must open these ports on your clients if you want to manage them. If you want to install Symantec AntiVirus on clients remotely, you must also open TCP ports 139 and 1024-5000 on those clients before installation.

Symantec AntiVirus servers also use TCP ports 2967 and 1024-5000 for almost all communications with Symantec AntiVirus clients, which support virus definitions updates, and so forth. Some services use random ports in this range, and some services use static ports. Symantec AntiVirus servers perform discovery by using TCP port 39263. If you want to install Symantec AntiVirus clients remotely, you must also open TCP ports 1024 - 4999 on your servers before installation. Legacy communications also require that UDP port 2967 be open on all computers.

Depending on your XP operating system and service pack, you might be able to open individual ports or specify programs that you want to trust to communicate through your firewall. Consult your Windows documentation for information on how to configure your firewalls.

Permitting remote software installation on Windows XP computers

By default, you cannot install Symantec AntiVirus software remotely on Windows XP computers that are installed in a workgroup. When Windows XP is installed in a workgroup, the Local Security Policy for Network Access Sharing and Security model is set to Guest instead of Classic. You must set this value to Classic to install software remotely on each server and client.

Note: This default does not apply to Windows XP computers that are installed in a domain.

To permit remote software installation on Windows XP computers

1. Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Local Policies** > **Security Options**.
2. Locate the policy for Network access: Sharing and Security model for local accounts.
3. Change the setting from Guest only - local users authenticate as Guest to Classic - local users authenticate as themselves.

About disabling other anti-security-risks programs

The current version of Symantec AntiVirus scans for security risks that are associated with adware and spyware, runs in real time, and might cause conflicts with similar products that other vendors offer. Before migrating antivirus servers and clients, disable or remove similar products that other vendors offer, especially those products that run in real time.

Chapter 3

Installing Symantec AntiVirus for the first time

This chapter includes the following topics:

- Before you install
- Installing the Symantec System Center
- Installing a management server from the Symantec System Center
- Configuring your server group
- Installing client software
- Testing antivirus capabilities

Before you install

If this is a first-time installation, you should install, configure, and test Symantec AntiVirus in a test environment on Windows computers. If you require support on NetWare servers, become familiar with the Windows installation first, and then test the installation on NetWare servers.

See "Installing Symantec AntiVirus servers" on page 103.

The installation and configuration procedures that follow describe how to install and configure Symantec AntiVirus on computers that are networked similarly to those shown in Figure 2-1.

See "Small deployment" on page 30.

The chapter about migration contains additional information about the SSL communications architecture that you might find useful.

See "About migrating to the SSL communications architecture" on page 68.

About client installation

The easiest way to install client software is to use the ClientRemote Install tool in the Symantec System Center. With this tool in a production environment, you can install to multiple clients at the same time without having to visit each workstation individually.

An advantage to remote installation is that users do not need to log on to their computers as administrators before the installation if you have administrator rights to the domain to which the client computers belong. When you install client antivirus software by using the Symantec System Center, the clients are automatically managed and associated with a server group.

Note: When you uninstall client software, the default password is `symantec`.

Installation sequence

The following list shows the order in which you install and configure management, server, and client software:

- Install the Symantec System Center.
- Install Symantec AntiVirus management server and configure it as a primary management server.
- Install Symantec AntiVirus client software.

Symantec System Center installation on server operating systems

The Symantec System Center installation is not permitted on supported Windows server operating systems when the following services are running:

- Terminal Services
- Fast Switching
- Remote Assistance
- Remote Desktop

To install the Symantec System Center on supported Windows server operation systems, you must disable these services. After installation, you can re-enable these services and use the Symantec System Center. In general, all server-side assistant services prevent the Symantec System Center installation.

Installing the Symantec System Center

The Symantec System Center is installed directly from the Symantec AntiVirus CD. Install the Symantec System Center to the computers from which you want to manage your antivirus protection.

Note: If you are installing the Symantec System Center on a computer that runs a supported Windows server operating system, you must first disable Terminal Services. You can re-enable Terminal Services after installation. Terminal Services (TermSrv.exe) prevents a successful installation. You can disable it from Task Manager or the Services dialog box in Administrator Tools.

In addition to the Symantec System Center, the following management components are installed by default:

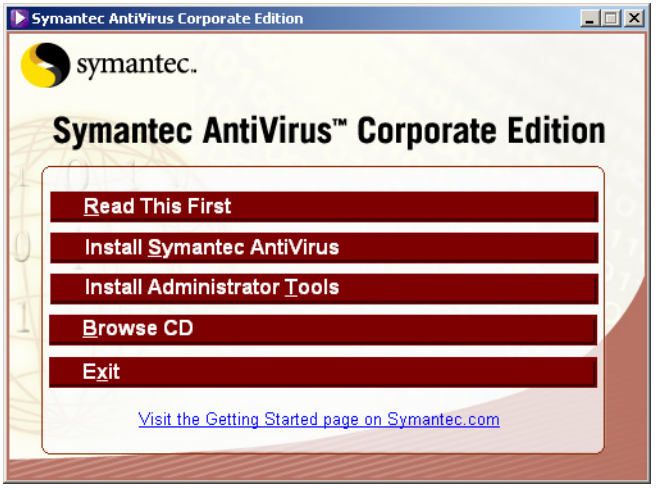
- Symantec AntiVirus snap-in: Required if you want to centrally manage antivirus protection.
- Symantec Client Firewall snap-in: Required if you want to centrally distribute firewall policy files.
- AV Server Rollout tool: Adds the ability to push the server installation to remote computers. This tool is also available on the Symantec AntiVirus CD.
- ClientRemote Install tool: Adds the ability to push the Symantec AntiVirus client installation to remote computers that run supported Microsoft Windows operating systems. This tool is also available on the Symantec AntiVirus CD.

If you elect not to install any of these management components with the Symantec System Center, you can run the Symantec System Center installation later and select them.

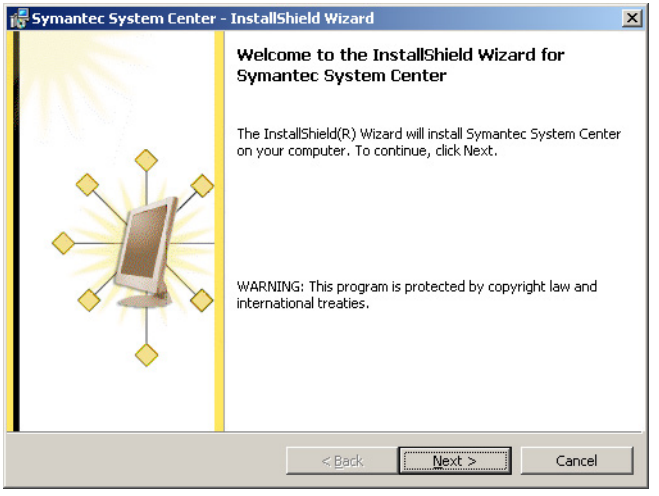
Note: If you are not managing Symantec Client Firewall clients, you do not need to install the Symantec Client Firewall snap-in. However, doing so will not cause any problems. Symantec Client Firewall is not included with Symantec AntiVirus Corporate Edition.

To install the Symantec System Center

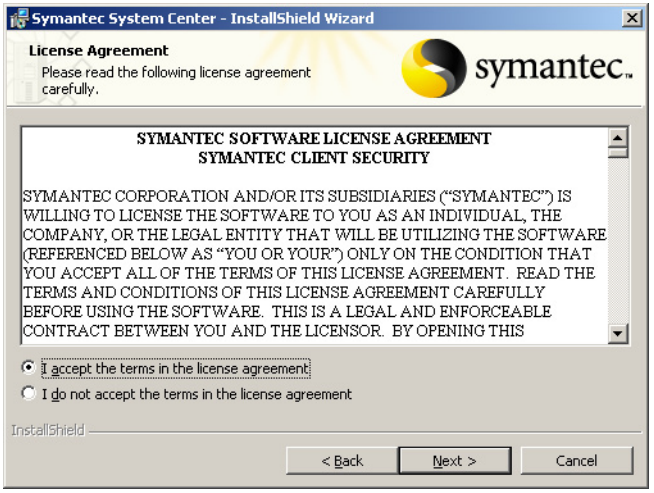
1 Insert the Symantec AntiVirus CD into the CD-ROM drive.



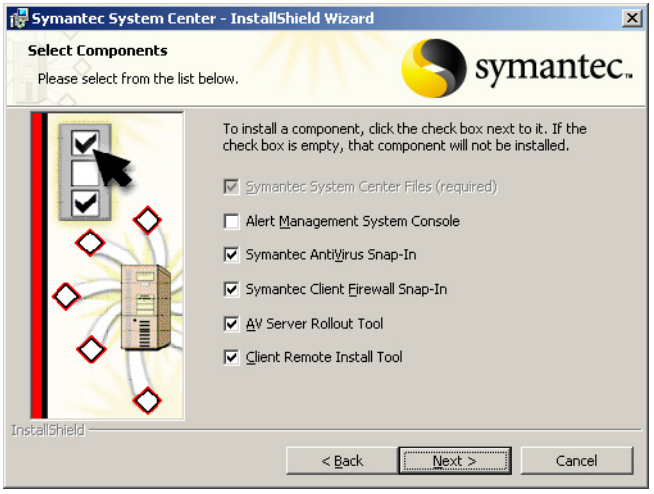
2 In the Symantec AntiVirus panel, click **Install Administrator Tools** > **Install Symantec System Center**.


Symantec System Center - InstallShield Wizard
Welcome to the InstallShield Wizard for Symantec System Center
The InstallShield(R) Wizard will install Symantec System Center on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

3 In the Welcome panel, click **Next**.


Symantec System Center - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
symantec.
SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC CLIENT SECURITY
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

4 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.


Symantec System Center - InstallShield Wizard
Select Components
Please select from the list below.
symantec.
To install a component, click the check box next to it. If the check box is empty, that component will not be installed.
Symantec System Center Files (required)
Alert Management System Console
Symantec AntiVirus Snap-In
Symantec Client Firewall Snap-In
AV Server Rollout Tool
Client Remote Install Tool
InstallShield
< Back
Next >
Cancel

If Microsoft Management Console 1.2 or later is not installed on the computer, a message indicates that you must allow it to install.

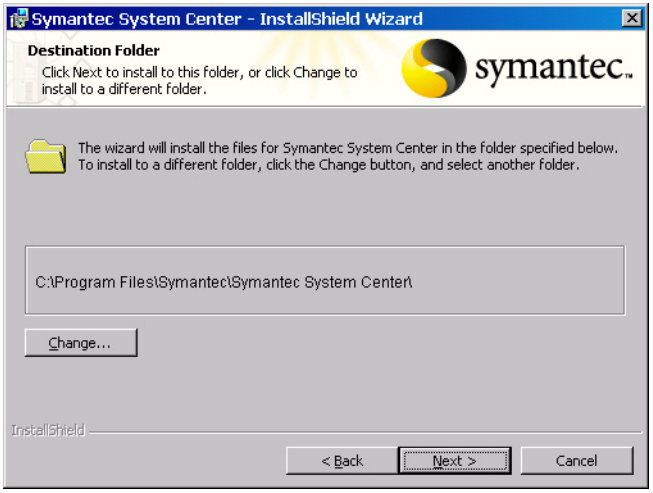
5 In the Select Components panel, check any of the following components that you want to install:

- Alert Management System Console
- Symantec AntiVirus Snap-In

- Symantec Client Firewall Snap-In
- AV Server Rollout Tool
- ClientRemote Install Tool

If these components are not present on the computer, all of them except Alert Management System Console are checked automatically.

6 Click **Next**.

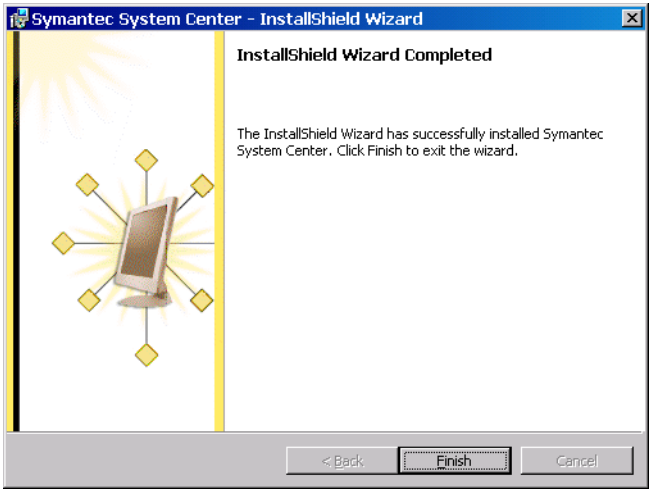

Symantec System Center - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
symantec.
The wizard will install the files for Symantec System Center in the folder specified below. To install to a different folder, click the Change button, and select another folder.
C:\Program Files\Symantec\Symantec System Center\
Change...
InstallShield
< Back
Next >
Cancel

7 In the Destination Folder panel, do one of the following:

- To accept the default destination folder, click **Next**.
- Click **Change**, locate and select a destination folder, click **OK**, and then click **Next**.

Symantec System Center - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
symantec.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

8 In the Ready to Install the Program panel, click **Install**.


Symantec System Center - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Symantec System Center. Click Finish to exit the wizard.
< Back
Finish
Cancel

9 In the InstallShield Wizard Completed panel, to close the wizard, click **Finish**.

10 When you are prompted to restart the computer, click **Yes**.

Installing a management server from the Symantec System Center

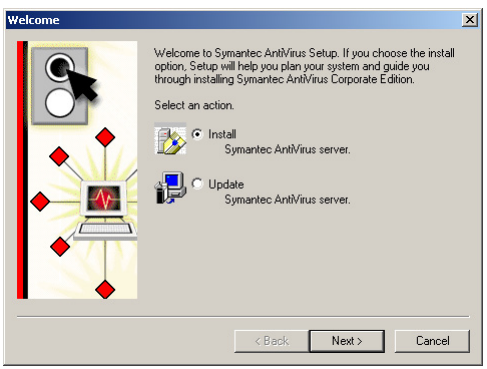
You can install a management server from the Symantec System Center, which is the easiest installation method. You can also install the server from the CD. When you install for the first time, you should install the server on the computer that contains the Symantec System Center.

Note: Do not deploy servers in a server group until you have created a server group, installed one server in the group, and made it the primary management server for the group.

As a best practice, always install a secondary management server in your server group for disaster recovery purposes. If you do not and your primary management server fails, you will not be able to access the server group from the Symantec System Center. If you do not create a secondary management server in your server group, back up the pki directory and all subdirectories. If your primary server becomes corrupt, you can re-create it if you have the backup files to restore. For details, refer to the Knowledge Base articles on the Symantec Web site.

To install a management server from the Symantec System Center

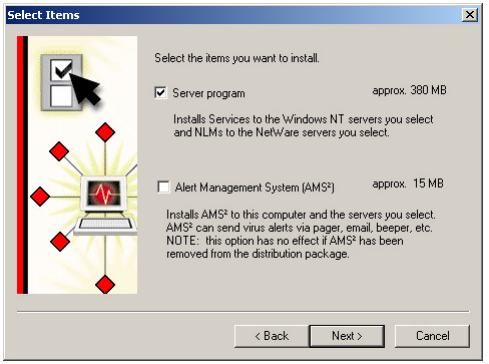
1. In the Symantec System Center console, in the left pane, expand **Symantec System Center**.
2. Click **Tools > AV Server Rollout**.


Welcome
Welcome to Symantec AntiVirus Setup. If you choose the install option, Setup will help you plan your system and guide you through installing Symantec AntiVirus Corporate Edition.
Select an action.
Install
Symantec AntiVirus server.
Update
Symantec AntiVirus server.
< Back
Next >
Cancel

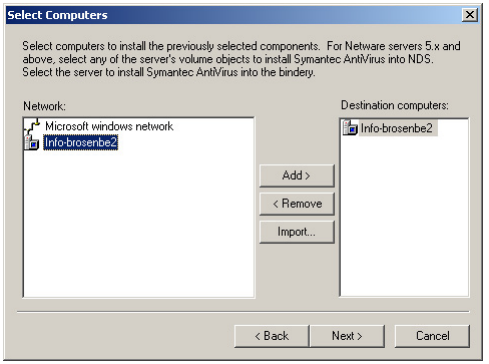
AV Server Rollout is available only if you selected the Server Rollout component when you installed the Symantec System Center. This component is selected for installation by default.

3 In the Welcome panel, click **Install Symantec AntiVirus server,** and then click **Next**.

4 In the License Agreement panel, click **I agree**, and then click **Next**.

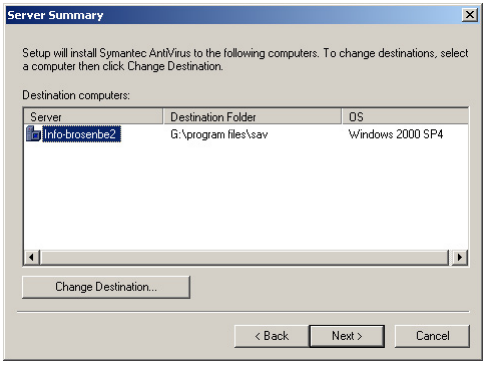

Select Items
Select the items you want to install.
Server program
approx. 380 MB
Installs Services to the Windows NT servers you select and NLMs to the NetWare servers you select.
Alert Management System (AMS²)
approx. 15 MB
Installs AMS² to this computer and the servers you select. AMS² can send virus alerts via pager, email, beeper, etc. NOTE: this option has no effect if AMS² has been removed from the distribution package.
< Back
Next >
Cancel

5 In the Select Items panel, ensure that Server program is checked, and then click **Next**.


Select Computers
Select computers to install the previously selected components. For Netware servers 5.x and above, select any of the server's volume objects to install Symantec AntiVirus into NDS. Select the server to install Symantec AntiVirus into the bindery.
Network:
Microsoft windows network
Info-brosenbe2
Destination computers:
Info-brosenbe2
Add >
< Remove
Import...
< Back
Next >
Cancel

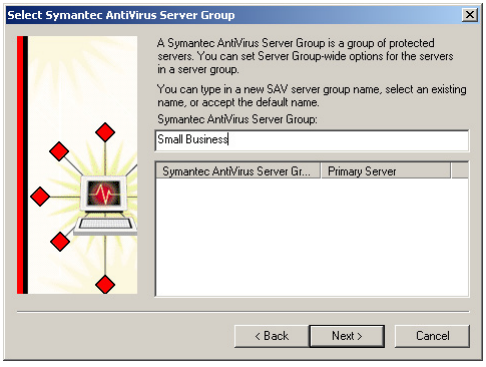
6 In the Select Computers panel, under Network, select the computer on which you installed the Symantec System Center, and then click **Add**.

7 Click **Next**.



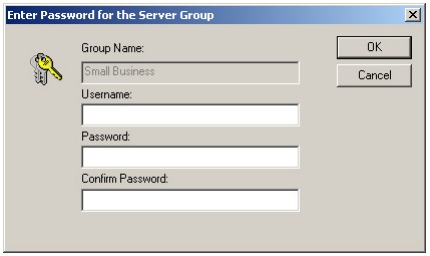
8 In the Server Summary panel, do one of the following:

- To accept the default Symantec AntiVirus installation path, click **Next**.
- To change the path, select a computer, and then click **Change Destination**. In the Change Destination dialog box, select a destination, click **OK**, and then click **Next**.

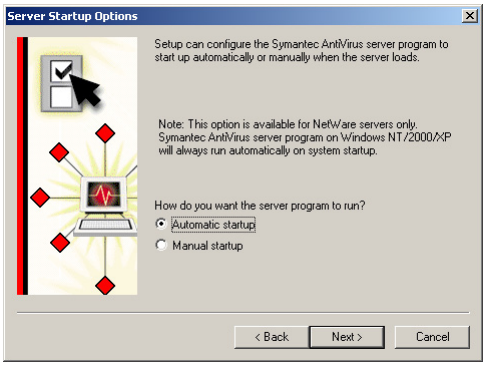

Select Symantec AntiVirus Server Group
A Symantec AntiVirus Server Group is a group of protected servers. You can set Server Group-wide options for the servers in a server group.
You can type in a new SAV server group name, select an existing name, or accept the default name.
Symantec AntiVirus Server Group:
Small Business
Symantec AntiVirus Server Gr...
Primary Server
< Back
Next >
Cancel

9 In the Select Symantec AntiVirus Server Group panel, under Symantec AntiVirus Server Group, type a name for a new server group, and then click **Next**.

10 In the Setup Message panel, click **Yes**.



11 In the Enter Password for the Server Group panel, type a user name, type and retype a password for the user name, and then click **OK**.
The user name that you type is the user name that administers the server group.


Server Startup Options
Setup can configure the Symantec AntiVirus server program to start up automatically or manually when the server loads.
Note: This option is available for NetWare servers only. Symantec AntiVirus server program on Windows NT/2000/XP will always run automatically on system startup.
How do you want the server program to run?
Automatic startup
Manual startup
< Back
Next >
Cancel

12 In the Server Startup Options panel, click **Automatic startup**, and then click **Next**.

13 In the Using the Symantec System Center Program panel, click **Next**.

14 In the Setup Summary panel, read the message, and then click **Finish**.

15 In the Setup Progress panel, view the status of the server installation, and then click **Close** when the installation is finished.

16 Close the Symantec System Center, save settings when you are prompted, and then restart the computer.

Configuring your server group

If you configure your server group before you install new clients, the clients are automatically configured to include virus definitions update and scanning schedules.

Configuring your server group involves the following tasks:

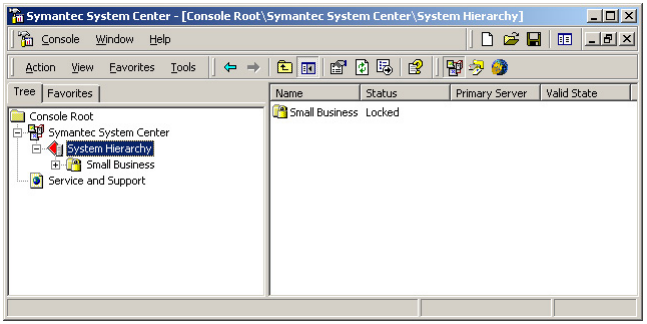
- Configuring a primary management server
- Protecting your server group root certificate private key
- Configuring updates and protection

Configuring a primary management server

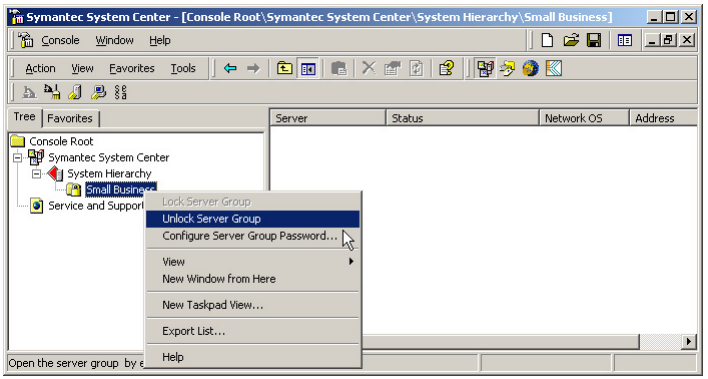
Every server group requires one primary management server. This server controls all other servers and clients in the server group. You cannot install clients from the Symantec System Center without configuring a primary management server.

To configure a primary management server

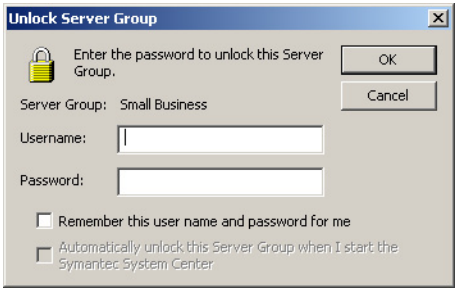
1. Start the Symantec System Center.
2. In the Symantec System Center console, in the left pane, expand **Symantec System Center > System Hierarchy**.



3 Right-click the server group that you created when you installed the antivirus server.



4 Click **Unlock Server Group**.

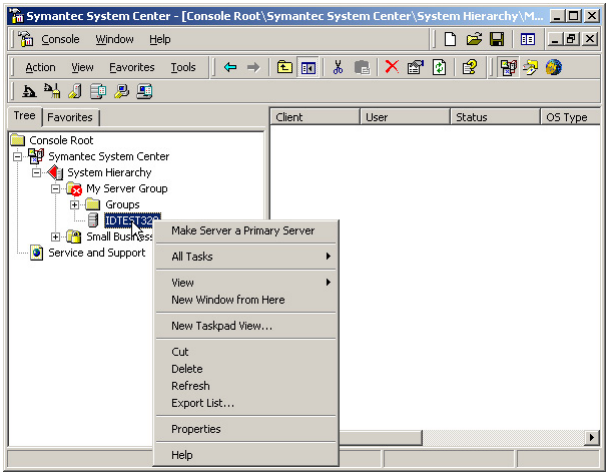

Unlock Server Group
Enter the password to unlock this Server Group.
OK
Cancel
Server Group: Small Business
Username:
Password:
Remember this user name and password for me
Automatically unlock this Server Group when I start the Symantec System Center

5 In the Unlock Server Group dialog box, do the following:

- In the Username box, type the user name that you entered when you installed the antivirus server.
- In the Password box, type the password that you entered when you installed the antivirus server.

6 Click **OK**.

7 In the left pane, right-click the computer name of the antivirus server.



8 Click **Make Server a Primary Server**.

9 In the prompt, click **Yes**.

10 On the main menu bar, click **Console > Save**.

Protecting your server group root certificate private key

The act of making a management server a primary server creates a server group root certificate that is in the <Drive:>\Program Files\SAV\pki\roots directory on the primary management server. This certificate was created by using a private key in the <Drive:>\Program Files\SAV\pki\private-keys directory on the primary management server.

The following examples show server group root certificate and private key naming conventions:

- <server-group-guid>.<counter>.servergroupca.cer
- <server-group-guid>.<counter>.servergroupca.pvk

The following examples show actual names for a certificate and private key:

- 4930435c2aa91e4abb4e6c9d527eb762.0.servergroupca.cer
- 4930435c2aa91e4abb4e6c9d527eb762.0.servergroupca.pvk

The server group root private key is used only to add new servers to a server group, so you should safely archive the key after you set up a server group with a primary management server, and add at least one secondary server. The key is not necessary for high-volume activity, such as adding clients and authenticating users.

If you promote an existing secondary server to a primary management server, and if you have not removed the private key from the original primary management server, the key is not automatically copied to the new primary. To add new secondary servers to the server group after you promote a new primary, you must install the private key on the new primary management server.

Warning: Do not lose this private key.

For more information about certificates, refer to the *Symantec AntiVirus Reference Guide* in the Docs directory on your installation CD.

Configuring updates and protection

By configuring your updates and protection before you install your clients, you automatically configure how clients protect against threats and get updated virus definition files during installation.

Configuring updates and protection involves the following tasks:

- Configuring VDTM for a server group
- Configuring scan schedules
- Configuring Auto-Protect scans

Configuring VDTM for a server group

The easiest way to keep servers and clients updated with the latest virus definitions is to use the Virus Definition Transport Method (VDTM). To use VDTM, you configure the primary management server in a server group to retrieve the latest virus definitions from either Symantec or an internal LiveUpdate server, and the definitions automatically propagate to all other servers and clients in the group.

Note: After you create a server group, VDTM by default is configured on the primary management server to randomly distribute virus definitions to clients every week between Thursday and Friday, within 480 minutes of 8:00 PM. If this schedule is satisfactory, you do not need to configure VDTM.

With VDTM, the other servers and clients in the group do not access the Internet, which preserves Internet gateway bandwidth. Typically, the internal LiveUpdate server is used only in very large networks to preserve additional Internet gateway bandwidth when you have a large number of primary servers that access the Internet.

To configure VDTM for a server group

1. In the Symantec System Center console, right-click a server, and then click **All Tasks > Symantec AntiVirus > Virus Definition Manager**.
2. In the Virus Definition Manager dialog box, do the following:
   - Under How Servers Retrieve Virus Definitions Updates, click **Update the Primary Server of this Server Group only**.
   - Under How Clients Retrieve Virus Definitions Updates, click **Update virus definitions from parent server**.
3. Click **Configure**.
4. In the Configure Primary Server Updates dialog box, click **Source**.
5. In the Setup Connection dialog box, in the Update definition file via list, click **LiveUpdate (Win32)/FTP(NetWare)**, and then click **OK**.
6. In the Configure Primary Server Updates dialog box, do both of the following:
   - Click **Update Now** to retrieve the virus definitions files from the primary management server immediately.
   - Click **Schedule For Automatic Updates**, click **Schedule**, and then specify a frequency and time when the server will check for updates on the primary management server.
7. Click **OK** until you return to the Symantec System Center main window.
8. Right-click **System Hierarchy**, and then click **Refresh.**

Configuring scan schedules

A scan schedule defines when all clients and servers in a server group scan hard disks for viruses and other threats. You should schedule these scans to run during off hours, when employees are least likely to work.

For details, refer to the *Symantec AntiVirus Administrator's Guide*.

To configure scan schedules

1. In the Symantec System Center console, right-click a server group.
2. Click **All Tasks > Symantec AntiVirus > Server Scheduled Scans**.
3. In the Scheduled Scans dialog box, on the Server Group Scans tab, click **New**.
4. In the Scheduled Scan dialog box, under Name, type a name for the scan.

5 Explore and configure other settings that are available with the Scan Settings and Advanced buttons.

6 Click **OK** until you return to the main window in the Symantec System Center console.

Configuring Auto-Protect scans

Auto-Protect scans files as you open them, and scans email attachments as they are sent and received. Servers support scanning the file system only. Clients support scanning the file system and email attachments. You can also set Threat Tracer for clients to identify computers that spread viruses to network shares.

For details, refer to the *Symantec AntiVirus Administrator's Guide*.

Configure Auto-Protect scans

When you configure Auto-Protect, you select a server group or server and configure scan settings.

To configure Auto-Protect scans for server file systems

1 In the Symantec System Center console, right-click the server group that you want to configure, and then click **All Tasks > Symantec AntiVirus > Server Auto-Protect Options**.

2 In the Server Auto-Protect Options dialog box, on the File System tab, check **Enable Auto-Protect**, and then click **Advanced**.

3 In the Server Auto-Protect Advanced dialog box, familiarize yourself with the various settings, and verify that the options under Threat Tracer are checked.

4 Click **OK**.

5 In the Server Auto-Protect Options dialog box, click **OK**.

To configure Auto-Protect scans for client file systems and email attachments

1 In the Symantec System Center console, right-click the server group that you want to configure, and then click **All Tasks > Symantec AntiVirus > Client Auto-Protect Options**.

2 In the Client Auto-Protect Options dialog box, on the File System tab, check **Enable Auto-Protect**, click the lock icon so that it is locked, and then click **Advanced**.

3 In the Auto-Protect Advanced Options dialog box, familiarize yourself with the various settings, and verify that the options under Threat Tracer are checked.

4 Click **OK**.

5 On the tab that corresponds with your email system, check **Enable Auto-Protect**. Your tab options are:

- Internet E-mail
- Lotus Notes®
- Microsoft® Exchange

6 Click **OK**.

Installing client software

You have two primary options for installing client software. You can install the software from the Symantec System Center, or you can install the software from the installation CD. You can also install client software by using Web-based installations and logon scripts.

See "Installing Symantec AntiVirus clients" on page 133.

This section includes the following topics:

- About disabling the Windows XP firewall
- Installing client software by using the Symantec System Center
- Installing client software from the CD

About disabling the Windows XP firewall

Windows XP with Service Packs 1 and 2 includes firewalls that can interfere with Symantec AntiVirus installation communications between servers and clients. If any of your servers or clients run Windows XP, you must disable the Windows XP firewall on them before you install Symantec AntiVirus client software.

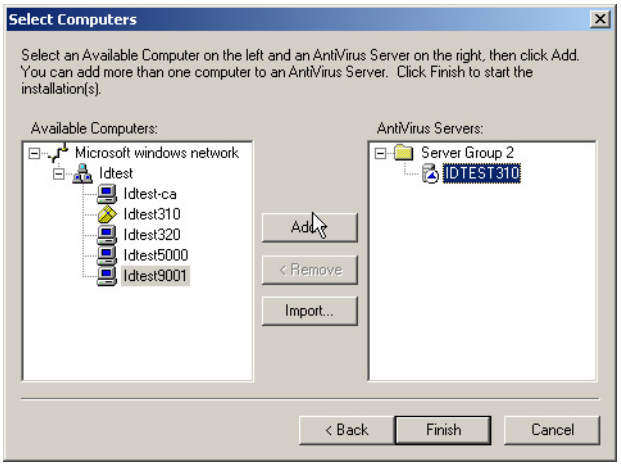
See "Disabling Windows XP firewalls" on page 39.

Installing client software by using the Symantec System Center

When you install clients from the Symantec System Center, the clients are automatically managed.

To install client software by using the Symantec System Center

1. In the Symantec System Center console, in the left pane, right-click the server group that you created when you installed the antivirus server.
2. If necessary, click **Unlock Server Group**, and then unlock the server group.
3. In the left pane, click the primary management server so that it remains highlighted.
4. On the Tools menu, click **ClientRemote Install**.
   ClientRemote Install is available only if you selected the ClientRemote Install tool when you installed the Symantec System Center. This component is selected for installation by default.
5. In the Welcome panel, click **Next**.
6. In the Select Install Source Location panel, click **Default location**, and then click **Next**.



7. In the Select Computers panel, under AntiVirus Servers on the right side, select a computer to act as the parent server (your primary management server).
8. Under Available Computers on the left side, expand **Microsoft windows network**, expand a group, and then select a client computer.
9. Click **Add**.
   The client computer moves under the AntiVirus parent server in the right pane.
10. Continue selecting and adding client computers until all of the clients that you want to manage are added, and then click **Finish**.

11 In the Status of Remote Client Installation(s) panel, when the remote installation is finished, click **Done**.

12 After a few minutes, in the Symantec System Center console, on the main menu bar, click **Actions > Refresh**.
The client computer appears in the right pane when the client software is fully installed, which may take up to a minute.

13 On the main menu bar, click **Console > Save**.

Installing client software from the CD

You can install the client software from the Symantec AntiVirus CD. The following procedure shows how to install the software on one client. You can install software on single computers, and you can deploy the software on multiple clients from the CD.

To install client software from the CD

1 Insert the Symantec AntiVirus CD into the CD-ROM drive.

2 In the Symantec AntiVirus panel, click **Install Symantec Client Security**, and then in the next panel click **Install Symantec Client Security**.

3 In the Welcome panel, click **Next**.

4 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.

5 In the Client Server Options panel, click **Client Install**, and then click **Next**.

6 In the Setup Type panel, click **Complete**, and then click **Next**.

7 In the Network Setup Type panel, click **Managed**, and then click **Next**.

8 In the Select Server panel, do one of the following:

- Next to Server Name, type the host name of the primary antivirus server that you installed and configured.
- Click **Browse**, select the primary antivirus server that you installed and configured, and then click **OK**.

9 Click **Next**.

10 In the Ready to Install the Program panel, click **Install**.

11 In the Installing Symantec Client Security panel, when the installation is finished, click **Finish**.

Note: The \Tools\PolicyFiles folder on the installation CD contains sample firewall policy files that you can test with, one of which supports Active Directory.

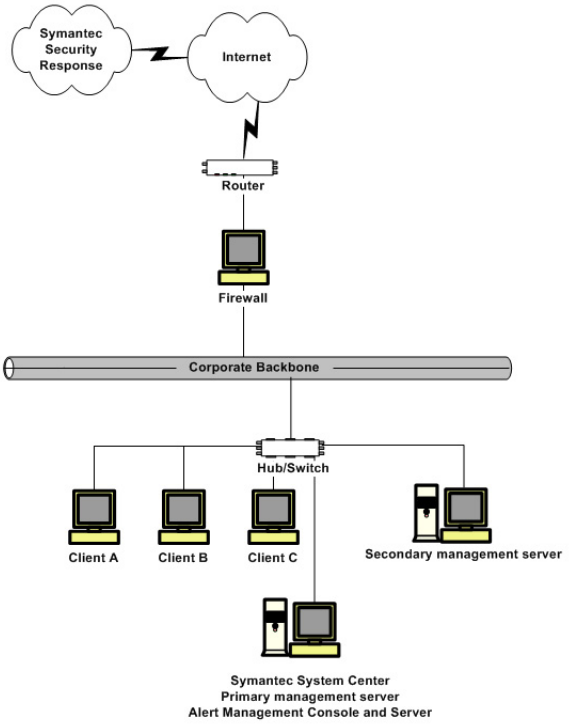
For details, refer to the *Symantec AntiVirus Administrator's Guide*.

Testing antivirus capabilities

Before rolling out Symantec AntiVirus servers and clients on a production network, you should experiment with antivirus detection in a controlled test environment to become familiar with alerts and log entries.

Figure 3-1 shows one way to configure a test environment.

Figure 3-1 Sample test environment



This test environment contains three clients, one primary management server, and one secondary management server for disaster recovery purposes. The Symantec System Center and the Alert Management Server and Console are also installed on the primary management server.

Configure a shared directory on one of the clients, and then mount the share on one of the other clients. To test email virus protection, configure the clients to send and receive supported email types with different accounts.

Finally, before you test antivirus detection, download the latest antivirus test file Eicar.com from www.eicar.org onto a floppy disk or some other transportable media.

Note: The reason that some of the following procedures instruct you to disable file system Auto-Protect is that Auto-Protect will delete or quarantine Eicar.com before you can complete your test.

Testing antivirus configuration

To test antivirus configuration, do the following:

- Unlock the Auto-Protect option for clients. Some tests require you to disable Auto-Protect.
  See "Configuring Auto-Protect scans" on page 59.
- In the Symantec System Center console, right-click your primary management server and view the antivirus log files. You should see entries related to configuring Auto-Protect, virus definition updates, and scan schedules.

Testing Auto-Protect

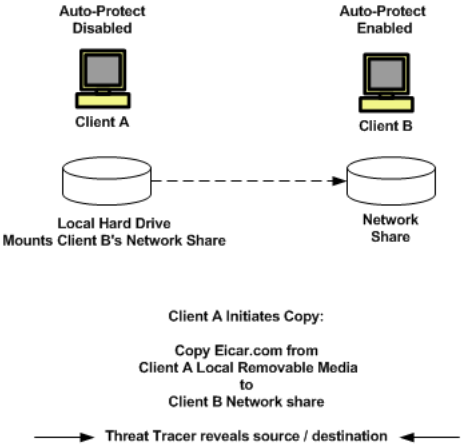
To test Auto-Protect, do the following:

- Enable file Auto-Protect on one of the clients, if it is not already enabled. Insert the removable media that contains Eicar.com into the client computer, and attempt to copy Eicar.com to the local hard drive. A virus notification alert appears.
- Disable file Auto-Protect (keep email Auto-Protect enabled) on one of the clients, attach Eicar.com to an email message, and send the email to an account that you can access on one of the other clients that has file and email Auto-Protect enabled. Open the email on the targeted client that runs in full Auto-Protect mode. A virus notification alert appears.

Testing Threat Tracer

To test Threat Tracer, do the following:

- On the client (for example, client A) that mounted the other client's shared directory (for example, client B), disable file system Auto-Protect, insert the removable media that contains Eicar.com, and copy the file to the shared directory on the other client (for example, client B). A virus notification alert appears. The following illustration shows this configuration.



- Refresh the Symantec System Center user interface, right-click the client that shares the directory (for example, client B), and then click **All Tasks > Symantec AntiVirus > Logs > Threat History**. Locate the EICAR Test string threat, right-click the threat, click **Properties**, and then the source computer name is identified.

Chapter 4

Migrating to the current version of Symantec AntiVirus

This chapter includes the following topics:

- About migration
- Supported and unsupported server and client migration paths
- Symantec System Center upgrade scenarios
- Upgrading the Symantec System Center
- Migrating management servers
- Migrating client software
- About migrating LiveUpdate servers

About migration

Symantec AntiVirus provides a seamless upgrade from earlier versions of Symantec antivirus products, which helps to minimize risk and continually increase the quality of security tools available to administrators. The Symantec AntiVirus client and server installation programs use Microsoft Windows Installer (.msi) technology, which provides flexibility, a smaller deployment size, in-field patching, and a variety of deployment options for migrating from earlier versions of Symantec products to the current version.

This chapter includes information on the supported and unsupported migration paths when upgrading to the current version of Symantec AntiVirus. For the most current information on migration, see the Symantec Knowledge Base.

Note: The user interface that appears when you install software from the CD and from the Symantec System Center console is relatively unchanged. Because you are migrating from one version to another, this chapter does not include step-by-step procedures for installing software.

Before you begin migration, read and understand the following topics:

- About migrating to the SSL communications architecture
- Disable security risk programs from other vendors
- How migration works
- Steps to migrating to the current version

About migrating to the SSL communications architecture

This version of Symantec AntiVirus uses SSL and digital certificates to provide secure communication paths and authentication between the Symantec System Center, servers, and clients. The impact on Symantec AntiVirus network management administration tasks is minimal.

However, senior-level administrators who install and configure Symantec AntiVirus servers should understand the relationship between private keys and digital certificates. Furthermore, you are occasionally prompted to copy certificates when you unlock a new server group or a server group that contains a migrated primary management server from the Symantec System Center.

For example, when you unlock a server group that contains a migrated primary management server for the first time with this version of the Symantec System Center console, you are prompted to copy the server group root certificate to the computer on which you installed this version of the Symantec System Center console. For details about SSL, certificates, and how Symantec AntiVirus implements certificates, refer to the *Symantec AntiVirus Reference Guide*.

First-time and existing customers should understand the following information:

- You should securely remove the server group private key from the \pki\private-keys directory on the primary management server after you create a primary management server and all secondary management servers. Copy the key to removable media, and then delete the key from the \pki\private-keys directory on the primary management server and from the Recycle Bin. Optimally, use a secure delete utility.

- If you remove the server group private key after you configure a primary management server, you must restore the private key to the primary management server before you can add secondary management servers to the server group.
- If you promote a secondary management server to a primary management server, and if the server group private key is on the primary management server, the key is not copied to the newly promoted primary management server as a security precaution. You must restore the server group private key to the newly promoted primary management server before you can add secondary management servers to the server group.
- You must never lose your server group private key.
- By default, the system clocks of all management console computers, servers, and clients must be within the default of 24 hours plus or minus of the system time on the primary management server. If this time requirement is not met, servers and clients will not authenticate the Symantec System Center logged on user and communications will fail. The plus time value is the value that is specified for the time validity of the login certificate. You can change both of these values by using the Configure Login Certificate Settings dialog box in the Symantec System Center.
- All communications (except one) between clients and servers now occur over TCP, while legacy communications continue to occur over UDP. The communications exception is that Discovery still occurs over UDP port 38,293.
- When you migrate a legacy primary management server to this version of Symantec AntiVirus, and if its server group contains legacy servers and clients, the migrated primary management server will continue to support legacy servers and clients over UDP.
- New server groups now authenticate with a user name and password, while legacy server groups authenticate with a password only. During the first server migration in a server group, you are prompted to type a user name. The name that you enter is the user name that you use to unlock the legacy server groups. The password that you use to unlock the legacy server group remains the same. The default user name is admin.
- If you create a new server group and a new primary management server by using this version of Symantec AntiVirus, legacy support over UDP is disabled by default in that server group. You can enable legacy support in that server group by using the Server Tuning Options dialog box in the Symantec System Center.
- You cannot manage newly installed servers and clients with legacy server groups or legacy Symantec System Center consoles.

- All newly installed or upgraded Symantec System Center consoles must run on the new version of Symantec AntiVirus, on either a management server or a managed client.
- As you migrate clients to this version, consider creating a new server group or groups by using the new version of the Symantec System Center, migrating existing clients, and then dragging and dropping them to a new server group or groups.
- The NT Remote Install client installation option in the Symantec System Center has been renamed to ClientRemote Install.
- You must restart every management server that is migrated.

Disable security risk programs from other vendors

The current version of Symantec AntiVirus scans for security risks that are associated with adware and spyware, runs in real time, and might cause conflicts with similar products that other vendors offer. Before you migrate antivirus servers and clients, disable or remove similar products that other vendors offer, especially those products that run in real time.

How migration works

Migration occurs by overinstalling the new version of Symantec AntiVirus management servers and clients on computers that run the old version. You do not need to uninstall management servers and clients before you install the new version. The overinstall process saves legacy settings, uninstalls the legacy software, and then installs the latest version. Furthermore, server group migration will fail if you uninstall migration-supported legacy management servers and clients.

When you migrate a primary management server, the overinstall automatically detects that the server is primary, and migrates and configures it appropriately when you install from the CD and select Install Symantec AntiVirus.

When you migrate a secondary management server, the overinstall automatically detects that the server is secondary, and migrates and configures it appropriately when you install from the CD and select Install Symantec AntiVirus.

You cannot migrate the Symantec System Center console with an overinstall. You must uninstall the legacy version, and then install the new version. This process is called upgrading. When you upgrade the first instance of the Symantec System Center console in your network, you must uninstall the Symantec System Center console, overinstall one or more management servers

in a server group, and then reinstall the Symantec System Center console in a specific order.

When you migrate a client, the overinstall automatically detects the client, and migrates and installs it appropriately.

Steps to migrating to the current version

Migrating to the current version of Symantec AntiVirus includes the following steps:

- Create a migration plan.
  Before you begin to install the Symantec AntiVirus client, server, and administration upgrades, you should have a solid understanding of your network topology and a streamlined plan to maximize the protection of the resources on your network during the upgrade. Migrating your entire network to the current version rather than managing multiple versions of Symantec AntiVirus is strongly recommended.
- If legacy Quarantine Console or Server is installed on any server or client that you plan to migrate, uninstall the legacy software first.
- Upgrade the Symantec System Center.
  The first step in migration is to install at least one new version of the Symantec System Center in the server group that contains the computer that runs the Symantec System Center.
  This process involves uninstalling the legacy version of the Symantec System Center, upgrading the primary management server to the new version, upgrading the Symantec software that protects the computer that runs the Symantec System Center, and then installing the new version of the Symantec System Center.
- After you upgrade the initial instance of the Symantec System Center, you then migrate secondary management servers in the server group that contains the computer that runs the Symantec System Center.
- After all management servers in the server group are migrated, deploy the new version of Symantec AntiVirus to clients.
- Migrate servers and clients in other server groups by migrating the primary management server first, migrating the secondary management servers, and then migrating the clients. You can perform this server migration remotely from the new version of the Symantec System Center.

Supported and unsupported server and client migration paths

The following section lists the platforms that are supported and unsupported when migrating to the current version of Symantec AntiVirus.

If the migration of a program is supported, the Symantec AntiVirus setup program automatically detects the software, removes the legacy components and registry entries, and installs the new version. If the migration from a previous product is not supported, you must uninstall the program before you run the Symantec AntiVirus installation program.

In most cases, if you are migrating from a legacy antivirus program that is not included in the list of supported migration paths, the installation program will fail during the installation, the user is notified that the installation was unsuccessful, and the Windows Installer log is updated. However, in some cases, if you do not uninstall the unsupported product before you run the installation, the installation may appear to succeed, but the product may not function properly. You should always uninstall any antivirus program that is not included in the list of supported migration paths before attempting to install the current version.

Quit all other Windows programs before installing Symantec AntiVirus. Other active programs may interfere with the installation and reduce your protection.

After migrating from several of these supported platforms, the computers may need to be restarted before they will be protected by Symantec AntiVirus.

For the most up-to-date information on supported migration paths and potential migration issues, see the Symantec Knowledge Base.

Note: When migrating from Norton AntiVirus™ Corporate Edition version 7.6x to the current version of Symantec AntiVirus, you should migrate servers before you migrate clients. When clients are migrated first, but are connected to a parent server running 7.6x, the 7.6x client software attempts to install over the current client software.

Supported migration paths

Symantec AntiVirus can migrate seamlessly over the following products:

- Symantec AntiVirus Corporate Edition 8.0 and later
- Norton AntiVirus Corporate Edition 7.6 and later
- Symantec Client Security, all versions

For Symantec Antivirus Corporate Edition 9.0 and later and Symantec Client Security 2.0 and later, custom installation paths are preserved. For example, if you installed the product in C:\Abc\MyAntiVirus\, the latest product files are installed in this directory after migration. For all other versions, the legacy product is uninstalled from custom installation paths, and the latest product in installed in the default installation directory.

Unsupported migration paths

Symantec AntiVirus migration is not supported for the following products:

- Symantec AntiVirus 64-bit client, version 9.0
  Symantec AntiVirus 64-bit client version 10.0 does not support Intel® Itanium® 2 processors, which were supported in version 9.0.
- Symantec Client Firewall Administrator
- Norton AntiVirus
- Norton Internet Security™
- Antivirus products from other vendors

If Norton SystemWorks™ is detected when the Symantec AntiVirus setup program runs, Symantec AntiVirus will not install.

Unsupported migration of Administrator tools

Symantec AntiVirus migration is not supported for the following Administrator tools:

- Symantec System Center
- LiveUpdate Administrator
- Quarantine Server and Quarantine Console

You must uninstall previous versions of these tools, and then install the latest version.

Custom settings may be lost

If you are not migrating from a supported migration path, any custom settings that you have are not saved during the migration process. On supported platforms, custom settings on clients and servers are preserved during migration.

Settings that are preserved for supported platforms include the following:

- Scheduled scans and LiveUpdate sessions
- All scan options
- Symantec Client Firewall policy files
- All Auto-Protect options
- Custom exclusions and file extensions to scan
- LiveUpdate host files
- Symantec AntiVirus activity logs
- Quarantine forwarding information

Quarantine items are automatically migrated

If there are any items in Quarantine on Symantec AntiVirus clients or servers, they are migrated automatically to the Symantec AntiVirus Quarantine. However, if any items in Quarantine are determined by Symantec AntiVirus to be uninfected, they are deleted rather than migrated.

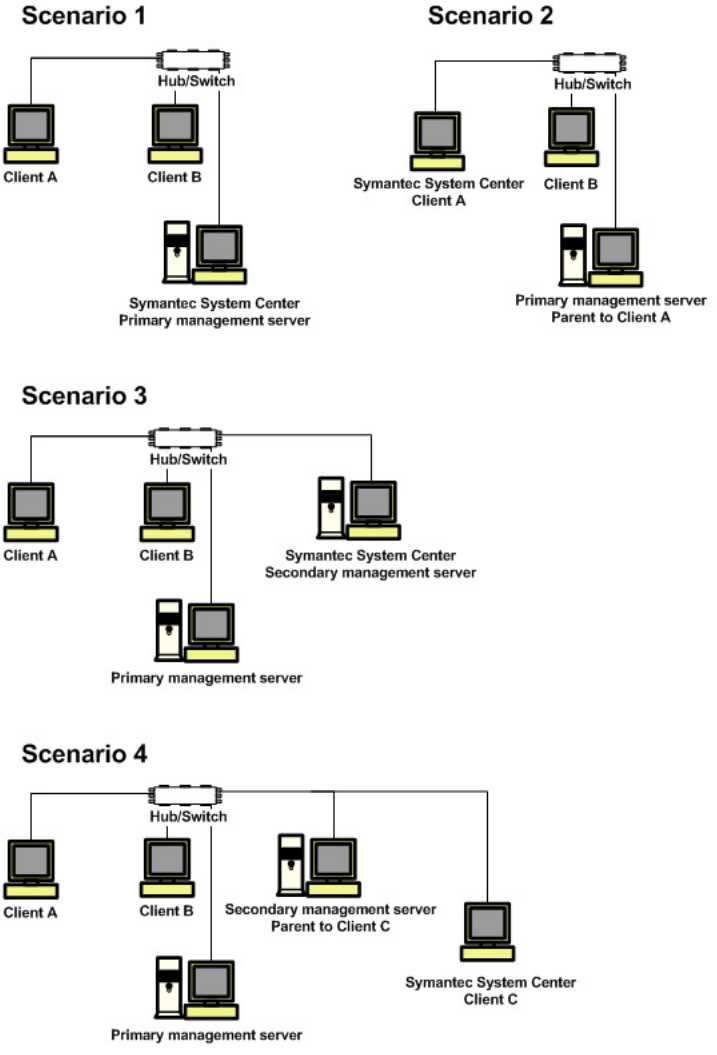
Symantec System Center upgrade scenarios

The goal of migration is to install a new version of the Symantec System Center and display your legacy server groups. An assumption is that the computer that runs the Symantec System Center is protected by and runs Symantec AntiVirus management server or client software, and that it is contained in a server group. Therefore, the computer that runs the Symantec System Center can be in one of the following four places in a server group:

- On the primary management server
- On a client that is managed by the primary server
- On a secondary management server
- On a client that is managed by a secondary server

Figure 4-1 illustrates these four locations, which equate to four possible scenarios for upgrading the first instance of the Symantec System Center in a server group.

Figure 4-1 Symantec System Center upgrade scenarios



Identify the scenario that matches the location of the computer that runs the Symantec System Center that you want to upgrade first. Each instance of the Symantec System Center that you want to upgrade must run on the new version of Symantec AntiVirus management server or client software, because you should always protect the computer that runs the Symantec System Center.

These upgrade scenarios apply to upgrading the first instance of a legacy Symantec System Center console in any server group. For subsequent upgrades of Symantec System Center consoles, you can uninstall the Symantec System Center just before you migrate the Symantec software that protects the computer that runs the Symantec System Center. You can then install the new version of the Symantec System Center.

Upgrading the Symantec System Center

The following topics describe how to upgrade the Symantec System Center:

- Before you upgrade the Symantec System Center
- Upgrading the Symantec System Center for your scenario
- Installing the Symantec System Center
- Unlocking the migrated server group

Before you upgrade the Symantec System Center

No matter which scenario you follow to upgrade the Symantec System Center, read the following information:

- If you plan to install the Symantec System Center on a computer that runs a supported Windows server operating system, disable Terminal Services. Terminal Services (TermSrv.exe) prevents a successful installation. You can disable it by using Task Manager or the Services dialog box in Administrator Tools. You can re-enable Terminal Services after installation.
- If legacy Quarantine Console or Server runs on a computer that you plan to migrate, uninstall this software before migration.
- Verify that the time clocks on all computers that you migrate are within 24 hours plus or minus of the time on the primary management server. You can change these values, if necessary, after the Symantec System Center upgrade by using the Configure Login Certificate Settings dialog box in the new Symantec System Center console. Symantec AntiVirus server and client communication will fail if you do not meet this requirement.
- The upgrade is complete only after you unlock your migrated server group from the Symantec System Center console and copy the server group root certificates to the directory structure that supports the Symantec System Center, when prompted.
- Select and follow the upgrade scenario that applies to your migration.
See "Symantec System Center upgrade scenarios" on page 74.

Upgrading the Symantec System Center for your scenario

Choose the scenario that applies to the location of the first primary management server in the first server group that you want to migrate, and follow that procedure for migration:

- Upgrading the Symantec System Center for scenario 1
- Upgrading the Symantec System Center for scenario 2
- Upgrading the Symantec System Center for scenario 3
- Upgrading the Symantec System Center for scenario 4

You must have physical access to each computer, and you must install by using the CD.

See "Symantec System Center upgrade scenarios" on page 74.

Upgrading the Symantec System Center for scenario 1

Do the following in sequence to upgrade the Symantec System Center when it runs on the legacy primary management server:

- Uninstall the legacy Symantec System Center.
- Overinstall the new version of Symantec AntiVirus server.
  See "Migrating the first management servers" on page 81.
- Install the new version of the Symantec System Center.
  See "Installing the Symantec System Center" on page 79.
- Unlock your migrated server group by using the Symantec System Center.
  See "Unlocking the migrated server group" on page 79.

Upgrading the Symantec System Center for scenario 2

Do the following in sequence to upgrade the Symantec System Center when it runs on a client that is managed by the legacy primary management server:

- On the computer that contains the client, uninstall the legacy Symantec System Center.
- On the computer that contains the legacy primary management server, overinstall the new version of Symantec AntiVirus server.
  See "Migrating the first management servers" on page 81.
- On the computer that contains the legacy client, overinstall the new version of Symantec AntiVirus client.
  See "Migrating clients by using the CD" on page 86.

- On the same computer, install the new version of the Symantec System Center.
  See "Installing the Symantec System Center" on page 79.
- Unlock your migrated server group by using the Symantec System Center.
  See "Unlocking the migrated server group" on page 79.

Upgrading the Symantec System Center for scenario 3

Do the following in sequence to upgrade the Symantec System Center when it runs on a secondary management server:

- On the computer that contains the secondary management server, uninstall the legacy Symantec System Center.
- On the computer that contains the legacy primary management server, overinstall the new version of Symantec AntiVirus server.
  See "Migrating the first management servers" on page 81.
- On the computer that contains the legacy secondary management server, overinstall the new version of Symantec AntiVirus server.
  See "Migrating the first management servers" on page 81.
- On the same computer, install the new version of the Symantec System Center.
  See "Installing the Symantec System Center" on page 79.
- Unlock your migrated server group by using the Symantec System Center.
  See "Unlocking the migrated server group" on page 79.

Upgrading the Symantec System Center for scenario 4

Do the following in sequence to upgrade the Symantec System Center when it runs on a client that is managed by the legacy secondary management server:

- On the computer that contains the client, uninstall the legacy Symantec System Center.
- On the computer that contains the legacy primary management server, overinstall the new version of Symantec AntiVirus server.
  See "Migrating the first management servers" on page 81.
- On the computer that contains the legacy secondary management server, overinstall the new version of Symantec AntiVirus server.
  See "Migrating the first management servers" on page 81.
- On the computer that contains the legacy client, overinstall the new version of Symantec AntiVirus client.
  See "Migrating clients by using the CD" on page 86.

- On the same computer, install the new version of the Symantec System Center.
  See "Installing the Symantec System Center" on page 79.
- Unlock your migrated server group by using the Symantec System Center.
  See "Unlocking the migrated server group" on page 79.

Installing the Symantec System Center

You can install the Symantec System Center console and components from the Symantec AntiVirus CD. The procedure assumes that you plan to install the Symantec System Center on a computer on which you installed the new version of Symantec AntiVirus server or client software.

To install the Symantec System Center console and components

1. From the Symantec AntiVirus CD, run Setup.exe.
2. On the Install Administrator Tools menu, click **Install Symantec System Center**.
3. Respond to the prompts until the installation completes.
4. Restart the computer.

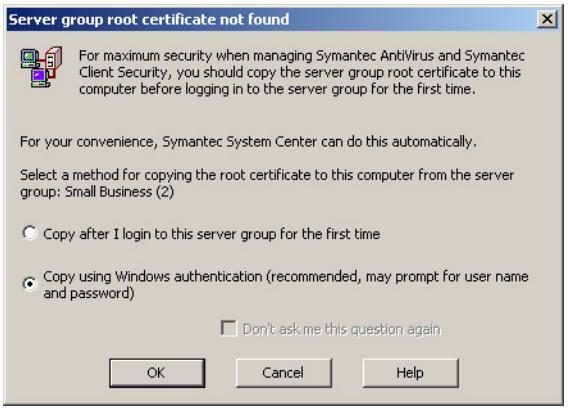
Unlocking the migrated server group

When you unlock a server group for the first time, a message appears that prompts you to copy the server group root certificate. This certificate is copied to the pki directory structure that supports the Symantec System Center.

To unlock the migrated server group

1. Start the Symantec System Center.

2 In the left pane, right-click the migrated server group, and then click **Unlock**.


Server group root certificate not found
For maximum security when managing Symantec AntiVirus and Symantec Client Security, you should copy the server group root certificate to this computer before logging in to the server group for the first time.
For your convenience, Symantec System Center can do this automatically.
Select a method for copying the root certificate to this computer from the server group: Small Business (2)
Copy after I login to this server group for the first time
Copy using Windows authentication (recommended, may prompt for user name and password)
Don't ask me this question again
OK
Cancel
Help

3 In the Server group root certificate not found dialog box, select either option, and then click **OK**.

4 In the Login dialog box, type the user name that you entered when you migrated the primary management server, type the password that you used to unlock the server group in the legacy version of the Symantec System Center, and then click **OK**.

Migrating management servers

There are several ways to install the Symantec AntiVirus server software to supported Windows and NetWare operating systems, including third-party deployment options such as Active Directory. Uninstalling servers is generally not required before you install the Symantec AntiVirus server software, provided that the server is not damaged.

Warning: Do not install multiple versions of Symantec AntiVirus server on a NetWare server. Either migrate or delete legacy server versions before you install the latest version.

The following topics describe how to migrate server software:

- Before you migrate management servers
- Migrating the first management servers
- About migrating subsequent servers
- Migrating from Symantec AntiVirus on NetWare platforms

- Preventing errors when the logon script is used
- About VPStart commands
- About migration from other server antivirus products

Before you migrate management servers

No matter which process that you follow to migrate servers, read and understand the following information:

- If a legacy instance of the Symantec System Center runs on a server that you plan to migrate, uninstall this software before migration.
- If a legacy instance of Quarantine Console or Server runs on a computer that you plan to migrate, uninstall this software before migration.
- Verify that the time clocks on all computers that you plan to migrate are within 24 hours plus or minus of the time on the primary management server.
- You must migrate servers in the following order:
  - Primary management server
  - Secondary management servers

Migrating the first management servers

You must migrate the first primary management server in the first server group that you want to migrate by installing the antivirus server software from the Symantec AntiVirus CD. If the initial instance of the Symantec System Center runs on a computer that is protected by Symantec AntiVirus client software, and has a secondary management server as a parent, the installation procedure also applies to that secondary management server.

Note: Do not install multiple management servers in a server group before you install and configure one primary management server in a server group.

To migrate the first management servers

1. From the Symantec AntiVirus CD, run Setup.exe.
2. In the Symantec AntiVirus panel, click **Install Symantec AntiVirus** > **Install Symantec AntiVirus**.

3 Follow and complete the prompts until you are prompted to enter a user name.

Symantec AntiVirus - InstallShield Wizard
Create Server Group User
Please enter information below
symantec.
The current Server Group information is being migrated. However a username for accessing the Server Group must be created.
Enter the username for the Server Group below.
Username
admin
InstallShield
< Back
Next >
Cancel

4 In the Create Server Group User panel, in the Username box, accept or change the user name that will be used to administer the existing server group, and then click **Next**.

5 Follow and complete the prompts until installation completes.

6 When installation completes, restart the computer.

About migrating subsequent servers

After you have migrated your first primary management server in your first migrated server group and accessed the primary management server in the Symantec System Center, you can migrate subsequent primary servers by using the deploy feature from the Symantec AntiVirus CD or by using the AV Server Rollout feature from the Symantec System Center. If you migrate a primary management server in another server group, migrate that server individually. You can then migrate multiple secondary management servers with deployment, but you must select Upgrade instead of Install.

See "Deploying the server installation across a network connection" on page 115.

Note: Do not install multiple management servers in a server group before you install and configure one primary management server in a server group.

Migrating from Symantec AntiVirus on NetWare platforms

The Symantec AntiVirus installation program detects earlier supported versions of Symantec AntiVirus on NetWare platforms. However, if you are migrating from a version that is not supported, you must manually uninstall Symantec AntiVirus on NetWare platforms from the servers to be migrated.

Migrate from supported and unsupported versions of Symantec AntiVirus on NetWare platforms

You can migrate from supported and unsupported versions of Symantec AntiVirus on NetWare platforms.

To migrate from a supported version of Symantec AntiVirus on NetWare platforms

1. From the Symantec AntiVirus CD, run Setup.exe.
2. In the Symantec AntiVirus panel, click **Install Symantec AntiVirus** > **Deploy AntiVirus Server**.
3. In the Welcome panel, click **Update**, and then click **Next**.
4. In the Select Computers panel, select the Computer Name, click **Add**, and then type the password for Server Group.
5. Click **Finish** to proceed with the update.
6. When the update process is finished, click **Close**, and then restart the computer.

To migrate from an unsupported version of Symantec AntiVirus on NetWare platforms

1. On the servers that you want to migrate that run Symantec AntiVirus on NetWare platforms, unload Symantec AntiVirus from the Symantec AntiVirus console on the server with VPStart /Remove.
   If you do not unload the Symantec AntiVirus NLM and you try to install the current version of Symantec AntiVirus, the installation will fail when you try to load VPStart /Install.
2. Remove the Symantec AntiVirus files from the server.
3. Use the NetWare Administrator (Nwadmin32.exe or Nwadmn95.exe) to remove the Symantec AntiVirus server object from the NDS tree.
4. Remove the Symantec AntiVirus load line from Autoexec.ncf, if necessary.
5. From the Symantec AntiVirus CD, run Setup.exe to install Symantec AntiVirus to your NetWare server.
6. When prompted to select Install or Update, click **Install**.

7 Select the server groups for the NetWare servers.
You can move the servers between server groups later.
All settings from the earlier version of Symantec AntiVirus are lost and must be reset in the Symantec System Center after Symantec AntiVirus is installed.
You can uninstall the Symantec AntiVirus client console program at your convenience by running its uninstallation item from the Symantec AntiVirus program group on the client computer.

Preventing errors when the logon script is used

The current version creates the SymantecAntiVirusAdmin and SymantecAntiVirusUsers NDS objects, but does not remove the NortonAntiVirusAdmin or NortonAntiVirusUsers NDS objects during migration. In addition, during migration, the container logon script is appended with the following section:

;###### Symantec AntiVirus Corporate Edition SECTION START ####### ...

;###### Symantec AntiVirus Corporate Edition SECTION END #######

To prevent errors that might occur when the logon script is used

1 Using NWAdmin or ConsoleOne, remove the following legacy section of the logon script:
;###### Norton AntiVirus Corporate Edition SECTION START ####### ...
;###### Norton AntiVirus Corporate Edition SECTION END #######

2 After you have completed the installation, you should move all users who were previously associated with the NortonAntiVirusUsers group to the new SymantecAntiVirusUsers group.

About VPStart commands

If you migrate from an earlier version of Symantec AntiVirus on a NetWare computer that used the option to start Symantec AntiVirus during startup, the installation file adds a new set of VPStart commands to autoexec.ncf, but does not remove the legacy VPStart commands that were used by the earlier version. To prevent errors, remove the duplicate commands by manually editing autoexec.ncf.

About migration from other server antivirus products

The Symantec AntiVirus installation requires all products that are not automatically uninstalled to be removed from the servers prior to installation.

Symantec AntiVirus also includes the Security Software Uninstaller that can detect and remove versions of antivirus software that are not included in the list of supported migration paths. For more information on using the Security Software Uninstaller, see the documentation provided for the tool in the \Tools\UNINSTLL directory on the Symantec AntiVirus CD.

After the antivirus program is uninstalled, the servers are treated like any other servers to which Symantec AntiVirus is rolled out.

Migrating client software

There are several ways to install the Symantec AntiVirus client software to supported Windows operating systems, including third-party deployment options such as Active Directory. Uninstalling previously existing clients is generally not required prior to installation of Symantec AntiVirus client, provided that the client is not damaged.

The following topics describe how to migrate client software:

- Before you migrate client software
- Migrating clients by using the CD
- Migrating clients by using the Symantec System Center
- Additional client migration methods
- How to determine parent servers and policy
- Other antivirus product client migrations

Before you migrate client software

No matter which process that you follow to migrate clients, read and understand the following information:

- If a legacy instance of the Symantec System Center runs on a client that you plan to migrate, uninstall this software before migration.
- If a legacy instance of Quarantine Console or Server runs on a computer that you plan to migrate, uninstall this software before migration.
- Verify that the time clocks on all computers that you plan to migrate are within 24 hours plus or minus of the time on the primary management server.

- If any of your clients run Windows XP, be sure to disable the firewalls that are included with Windows XP, including Service Pack 1 and Service Pack 2.
See "Disabling Windows XP firewalls" on page 39.
- The NT Client Install tool in the Symantec System Center is renamed to RemoteClient Install.

Migrating clients by using the CD

To migrate from an earlier version of Symantec AntiVirus, you can follow the standard installation procedure for installing a client.

To migrate clients by using the CD

1. From the Symantec AntiVirus CD, run Setup.exe.
2. In the Symantec AntiVirus panel, click **Deploy Symantec AntiVirus**.
3. Proceed with the upgrade process.

Migrating clients by using the Symantec System Center

To migrate from an earlier version of Symantec AntiVirus, you can deploy a client installation from the Symantec System Center.

To migrate clients by using the Symantec System Center

1. In the Symantec System Center console, in the left pane, click **System Hierarchy** or any object under it.
2. On the Tools menu, click **ClientRemote Install**.
   ClientRemote Install is available only if you selected the ClientRemote Install tool when you installed the Symantec System Center. This tool is selected for installation by default.
3. Continue the installation until complete.

Additional client migration methods

All of the client installation methods, when used to overinstall Symantec AntiVirus client software, migrate clients. In each case, automatic migration from earlier versions of Symantec AntiVirus occurs. Also, the clients inherit the policy that was set on the parent server.

See "About client installation methods" on page 135.

How to determine parent servers and policy

When Symantec AntiVirus is installed to servers, each server receives a full set of installation files for all supported platforms in the folder Program Files\Sav\Clt-inst on a Windows-based server and SYS:SAV\clt-inst on a NetWare server.

When the antivirus policy is set on the server, the policy settings are saved in the Grc.dat file. This file exists in all of the installation sets and is updated any time that the policy is changed. When Symantec AntiVirus is then installed to clients from these installation sets, the policy is carried to the clients with this file, along with the identification of the parent server.

When clients are migrated from earlier versions of Symantec AntiVirus, the folder to which that version is installed is used.

Note: When migrating to the current version of Symantec AntiVirus, migrate servers before you migrate clients.

Other antivirus product client migrations

Since the Symantec AntiVirus installation will not recognize the presence of other antivirus products, the products must be removed prior to the rollout.

Symantec AntiVirus includes the Security Software Uninstaller that can detect and remove versions of antivirus software that are not included in the list of supported migration paths. For more information on using the Security Software Uninstaller, see the documentation provided for the tool in the \Tools\UNINSTLL directory on the Symantec AntiVirus CD.

Note: The MIGRATESETTINGS switch is used whether or not a custom Cpolicy.xml file is included in the installation files. MIGRATESETTINGS has no affect on Grc.dat.

About migrating LiveUpdate servers

If you have already set up LiveUpdate FTP servers or UNC paths, there is no need to modify them. They will continue to be used the same way with Symantec AntiVirus.

When the Symantec System Center is installed, you have the option to install LiveUpdate Administrator as well. To continue to use an internal LiveUpdate server, install LiveUpdate Administrator to at least one of your supported

Windows servers. This lets you schedule LiveUpdate Administration Utility retrieval of packages directly from the Symantec System Center.

For details, refer to your *LiveUpdate Administrator's Guide* on the installation CD.

Chapter 5

Installing Symantec AntiVirus management components

This chapter includes the following topics:

- Before you install
- Symantec System Center installation
- Installing and configuring the Central Quarantine
- Installing and configuring the LiveUpdate Administration Utility
- Uninstalling Symantec AntiVirus management components

Before you install

Symantec AntiVirus management components include the following:

- Symantec System Center
- Central Quarantine
- LiveUpdate Administration Utility
- VPN Sentry

To use the management components, you must first install the Symantec System Center.

See "Installing the Symantec System Center" on page 45.

After you install the Symantec System Center, you can then install the Central Quarantine and LiveUpdate Administration Utility, and configure them with the Symantec System Center to protect your client computers.

Note: If you choose to install the Symantec System Center, Quarantine Server, or Quarantine Console from the individual installation folders on the Symantec AntiVirus CD, you should run Setup.exe rather than running the .msi installation package directly. Using Setup.exe ensures that all of the files that Windows Installer requires are installed on the target computer before the .msi installation package runs.

How to prepare for the Symantec System Center installation

Before you install the Symantec System Center, on the computer to which you are installing the Symantec System Center, you should uninstall the following:

- Any earlier versions of the Symantec System Center
- Any earlier versions of Symantec AntiVirus (including any versions of LANDesk® Virus Protect)

The Symantec System Center can manage earlier supported versions of Symantec AntiVirus, but the computer that is running the Symantec System Center must be using the current version of Symantec AntiVirus. You can install the Symantec System Center console to as many computers as you need to manage Symantec AntiVirus.

Symantec System Center installation and Terminal Services

The Symantec System Center installation is not permitted on supported Windows server operating systems when the following services run:

- Terminal Server and Services
- Fast Switching
- Remote Assistance
- Remote Desktop

Most server-side assistant services prevent the Symantec System Center installation. To install the Symantec System Center on supported Windows server operating systems, you must first stop these services, after which you can install the Symantec System Center. After installation, you can then restart and use these services.

Warning: The Symantec System Center will not work properly if two users who are logged on to the same system attempt to use the Symantec System Center at the same time.

Symantec System Center installation

Silent installation of the Symantec System Center is not supported. Note that after you install the Symantec System Center, you must restart the computer before you run the Symantec System Center.

If you install another instance of the Symantec System Center, and attempt to open detected server groups, you are prompted to copy certificates to the computer that runs that new instance. You must copy certificates when prompted.

Note: If you are installing the Symantec System Center on a computer that runs a supported Windows server operating system, you must first disable Terminal Services. You can re-enable Terminal Services after installation. Terminal Services (TermSrv.exe) prevents a successful installation. You can disable it from Task Manager or the Services dialog box in Administrator Tools.

See "Installing the Symantec System Center" on page 45.

Note: Installing this version of Symantec Client Firewall Administrator on computers that run legacy client software is unsupported. Migrate the legacy client software before you install Symantec Client Firewall Administrator.

Installing and configuring the Central Quarantine

The Central Quarantine is composed of the Quarantine Server and the Quarantine Console. The Quarantine Server and the Quarantine Console can be installed on the same or different supported Windows computers.

The Quarantine Server is managed by the Quarantine Console, which snaps in to the Symantec System Center. To manage the Central Quarantine from the Symantec System Center console, the Quarantine Console snap-in must be installed.

Installation of the Central Quarantine requires the following tasks:

- Installing the Quarantine Console snap-in
- Installing the Quarantine Server
- Attaching a management server to the Central Quarantine
- Configuring servers and clients to use the Central Quarantine

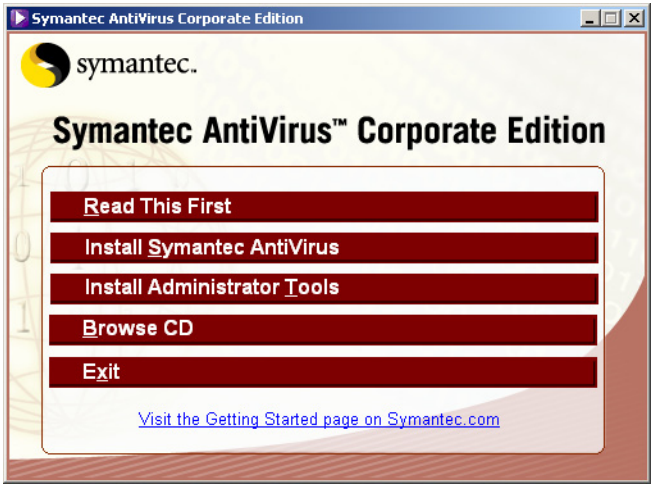
For complete information, see the *Symantec Central Quarantine Administrator's Guide* on the Symantec AntiVirus CD.

Installing the Quarantine Console snap-in

The Quarantine Console snap-in lets you manage submissions to the Quarantine Server.

To install the Quarantine Console snap-in

1 On the computer on which the Symantec System Center is installed, insert the Symantec AntiVirus CD into the CD-ROM drive.



If your computer is not set to automatically run a CD, you must manually run Setup.exe.

2 In the Symantec AntiVirus panel, click **Install Administrator Tools > Install Quarantine Console**.

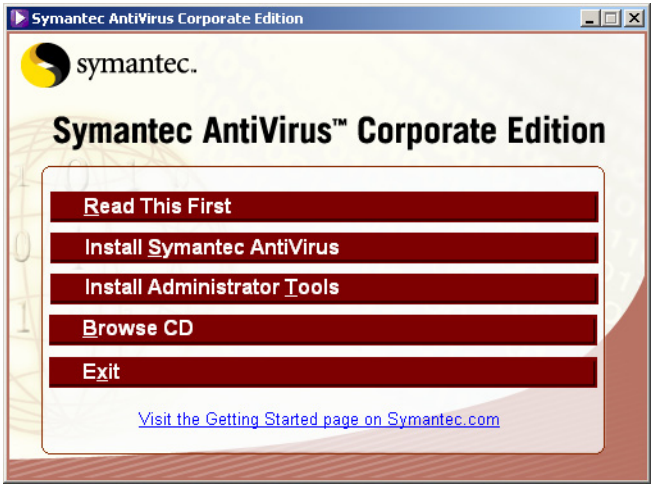
3 Follow the on-screen instructions.

Installing the Quarantine Server

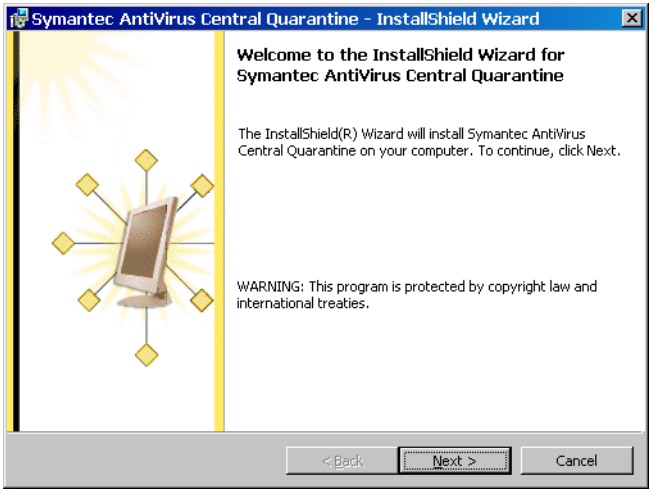
The Quarantine Server receives virus submissions.

To install the Quarantine Server

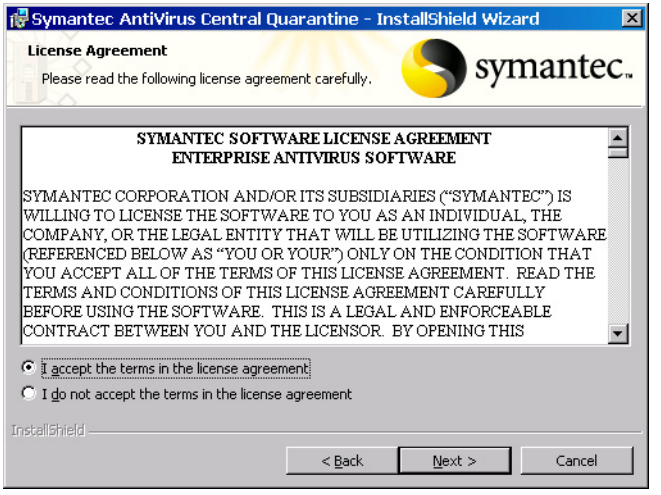
1 On the computer on which you want to install the Quarantine Server, insert the Symantec AntiVirus CD into the CD-ROM drive.



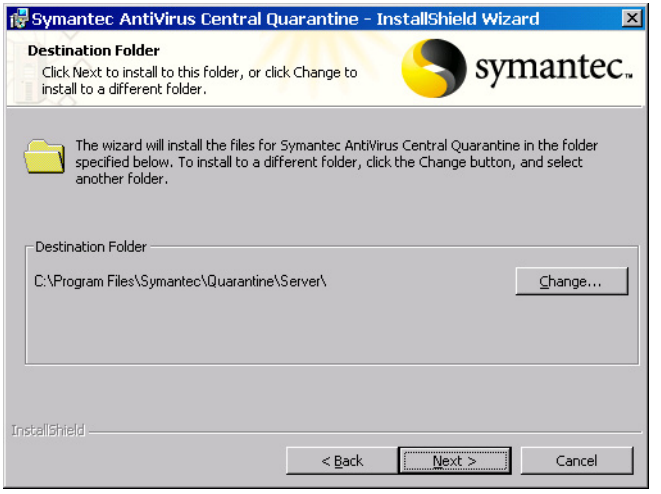
2 In the Symantec AntiVirus panel, click **Install Administrator Tools > Install Central Quarantine**.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
Welcome to the InstallShield Wizard for Symantec AntiVirus Central Quarantine
The InstallShield(R) Wizard will install Symantec AntiVirus Central Quarantine on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

3 In the Welcome panel, click **Next**.

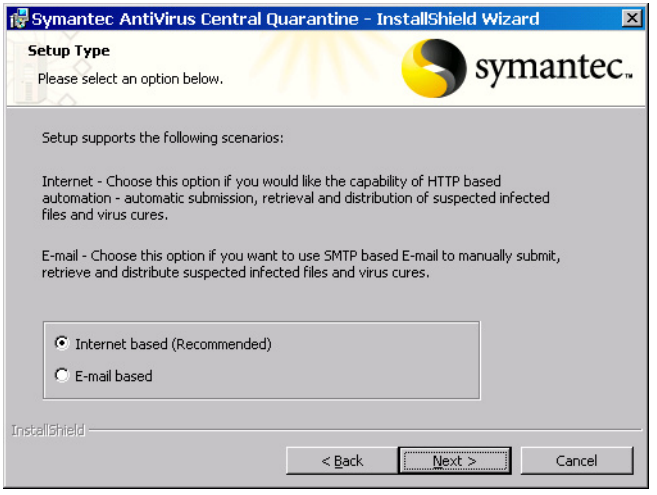

Symantec AntiVirus Central Quarantine - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
symantec.
SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

4 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
symantec.
The wizard will install the files for Symantec AntiVirus Central Quarantine in the folder specified below. To install to a different folder, click the Change button, and select another folder.
Destination Folder
C:\Program Files\Symantec\Quarantine\Server\
Change...
InstallShield
< Back
Next >
Cancel

5 In the Destination Folder panel, do one of the following:

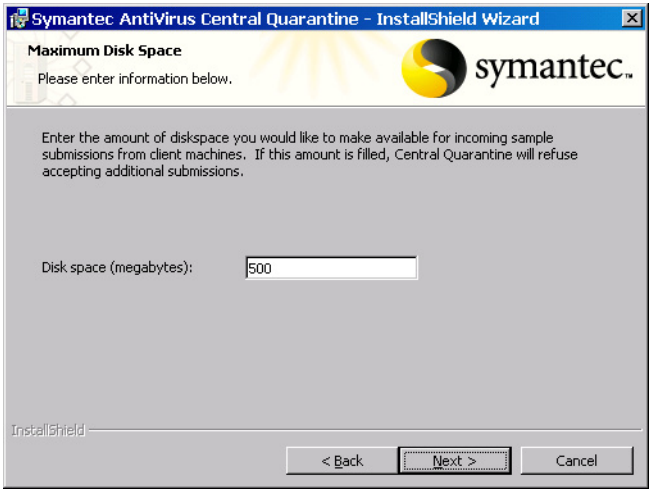
- To accept the default destination folder, click **Next**.
- Click **Change**, locate and select a destination folder, click **OK**, and then click **Next**.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
Setup Type
Please select an option below.
symantec.
Setup supports the following scenarios:
Internet - Choose this option if you would like the capability of HTTP based automation - automatic submission, retrieval and distribution of suspected infected files and virus cures.
E-mail - Choose this option if you want to use SMTP based E-mail to manually submit, retrieve and distribute suspected infected files and virus cures.
Internet based (Recommended)
E-mail based
InstallShield
< Back
Next >
Cancel

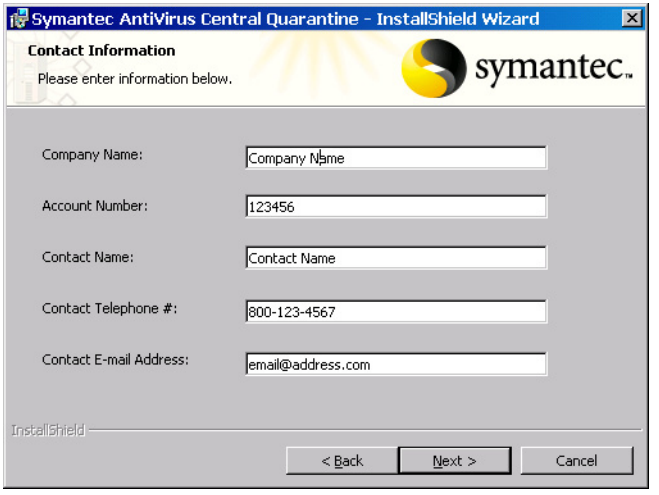
6 In the Setup Type panel, select one of the following:

- Internet based (Recommended)
- E-mail based

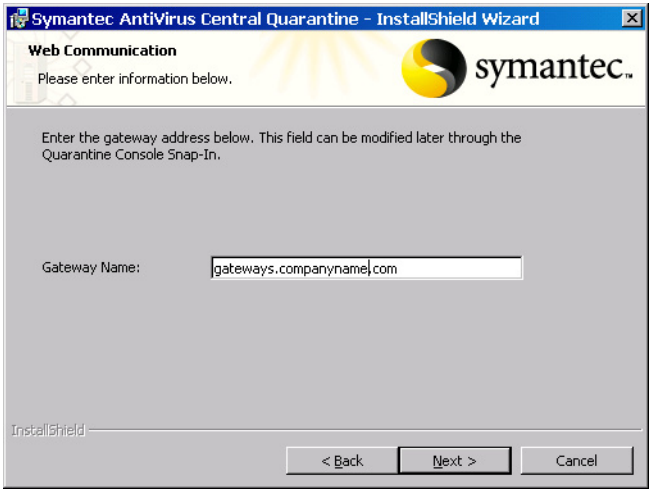
7 Click **Next**.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
Maximum Disk Space
Please enter information below.
symantec.
Enter the amount of diskspace you would like to make available for incoming sample submissions from client machines. If this amount is filled, Central Quarantine will refuse accepting additional submissions.
Disk space (megabytes):
500
InstallShield
< Back
Next >
Cancel

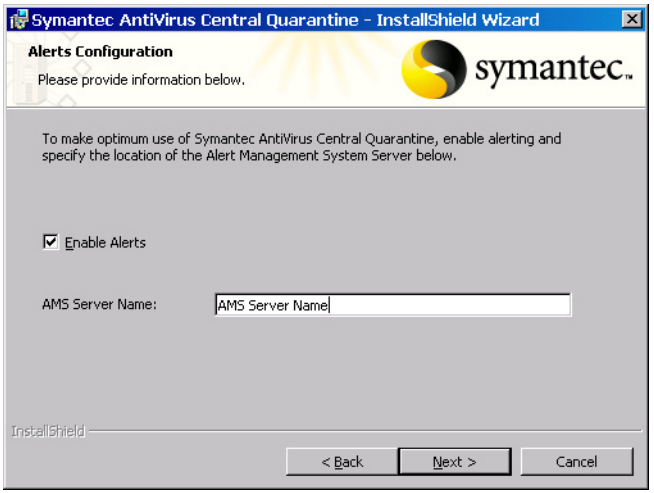
8 In the Maximum Disk Space panel, type the amount of disk space to make available on the server for Central Quarantine submissions from clients, and then click **Next**.



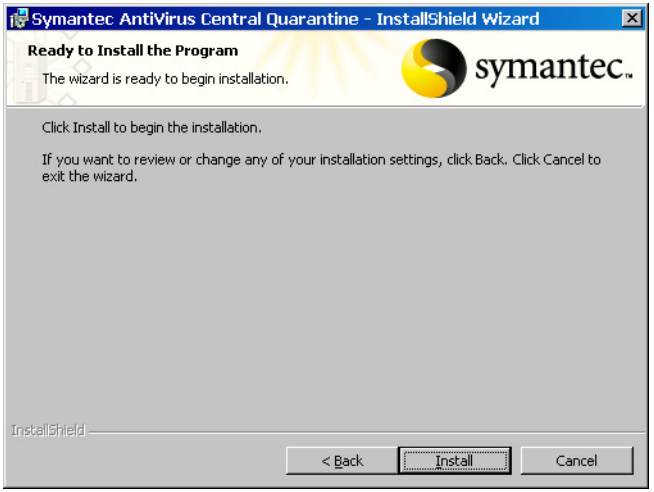
9 In the Contact Information panel, type your company name, your Symantec contact ID/account number, and contact information, and then click **Next**.



10 In the Web Communication panel, change the gateway address if necessary, and then click **Next**.
By default, the Gateway Name field is filled in with the gateway address.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
Alerts Configuration
Please provide information below.
symantec.
To make optimum use of Symantec AntiVirus Central Quarantine, enable alerting and specify the location of the Alert Management System Server below.
Enable Alerts
AMS Server Name:
AMS Server Name
InstallShield
< Back
Next >
Cancel

11 In the Alerts Configuration panel, check **Enable Alerts** to use AMS^2, type the name of your AMS^2 server, and then click **Next**.
You can leave this blank if no AMS^2 server is installed.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
symantec.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

12 In the Ready to Install the Program panel, click **Install**, and then follow the on-screen prompts to complete the installation.

13 Write down the IP address or host name of the computer on which you installed the Quarantine Server.
This information will be required when you configure client programs to forward items to the Central Quarantine.

Attaching a management server to the Central Quarantine

Attaching an antivirus server to the Quarantine Server enables you to submit infected files to the Quarantine server. For details on how to attach a server that is not on the same computer as the Quarantine server, see the *Symantec Central Quarantine Administrator's Guide* on the Symantec AntiVirus CD.

To attach an antivirus server to the Central Quarantine

1 Start the Symantec System Center.

2 In the left pane, right-click **Symantec Central Quarantine**, and then click **Attach to server**.

3 In the Select Computer panel, click **This computer**, and then click **Finish**.

4 On the Console menu, click **Save**.

Configuring servers and clients to use the Central Quarantine

You must configure all existing and future servers and clients in a server group to forward quarantined files to the Quarantine Server.

To configure servers and clients to use Central Quarantine

1 In the Symantec System Center console, in the left pane, right-click the server group that you created when you installed the antivirus server.

2 Click **Unlock Server Group**, and then unlock the server group.

3 Right-click the server group, and then click **All Tasks > Symantec AntiVirus > Quarantine Options**.

4 In the Symantec AntiVirus Management Snap-In dialog box, click **Yes**.

5 In the Quarantine Options dialog box, check **Enable Quarantine or Scan and Deliver**.

6 Under Server Name, type the host name of the local computer.

7 Under port, type the local port number to use.
The port number should be greater than 1024.

8 Click **OK**.

9 On the Console menu, click **Save**.

Installing and configuring the LiveUpdate Administration Utility

You can use the LiveUpdate Administration Utility to create a single download point for virus definitions and updates to Symantec products that use LiveUpdate. You can set up a LiveUpdate server on one or more Internet-ready computers to distribute updates across an internal local area network (LAN).

For more information, see the *LiveUpdate Administrator's Guide* on the Symantec AntiVirus CD.

To set up a LiveUpdate server with the LiveUpdate Administration Utility, and to set up servers to retrieve updates from the LiveUpdate server, complete the following tasks:

- Install the LiveUpdate Administration Utility.
  Configure the LiveUpdate Administration Utility scheduling from the Symantec System Center console to download updates from Symantec.
- Configure the LiveUpdate Administration Utility.
  Specify the packages to download and the directory to which the packages will be downloaded.
  If you have workstations that are connected to a UNC network location, the user who is logged on to the network must have access rights to the network resource. The user name and password that are supplied in the host file are ignored. With a Windows server, you can create a shared resource that all users are authorized to access (a NULL share). For more information on creating a NULL share, see the Microsoft Windows server documentation.
- Ensure that your FTP server, Web server, or UNC share is configured to share files from the download directory that you specified.
- In the Symantec System Center, do the following:
  - Configure LiveUpdate for the internal LiveUpdate server.
  - Configure other servers and clients to download virus definitions and program updates from the internal LiveUpdate server.
  - Schedule when you want LiveUpdate sessions to run.

Many administrators prefer to test virus definitions files on a test network before making them available on a production server. If you test your virus definitions files, test them on your test network. Once testing is complete, run LiveUpdate from your production network.

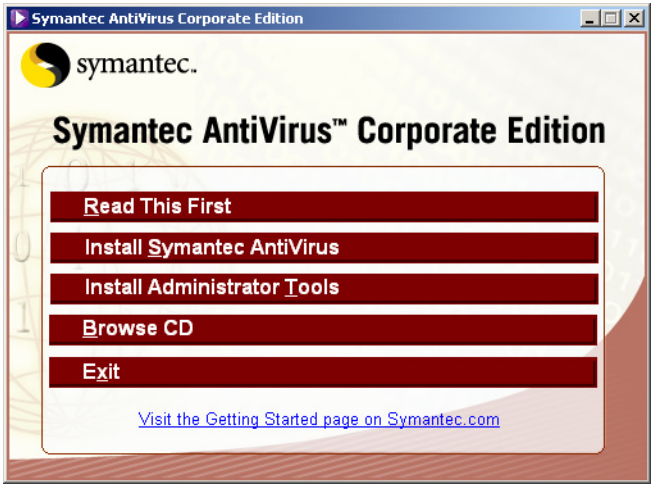
Install and configure the LiveUpdate Administration Utility

Install the LiveUpdate Administration Utility on a Windows computer that is running the server program, and then configure it.

For more information on using the LiveUpdate Administration Utility, see the *LiveUpdate Administrator's Guide* PDF on the Symantec AntiVirus CD.

To install the LiveUpdate Administration Utility

1 Insert the Symantec AntiVirus CD into the CD-ROM drive.



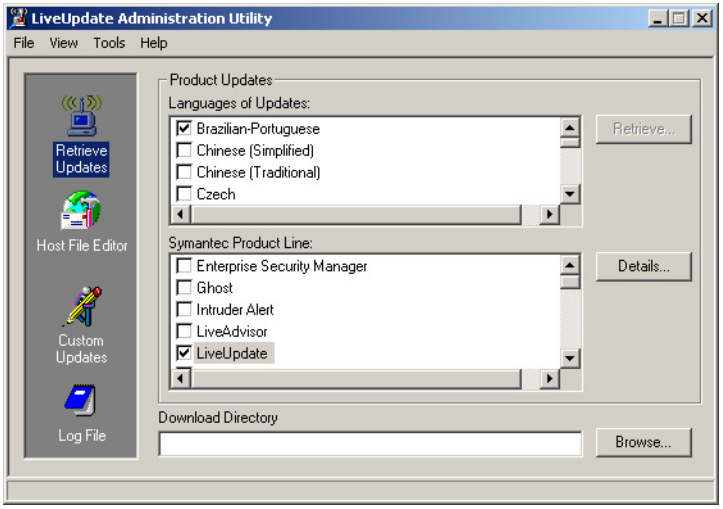
2 In the Symantec AntiVirus panel, click **Install Administrator Tools > Install LiveUpdate Administrator**.

3 Follow the on-screen instructions.

To configure the LiveUpdate Administration Utility

1 On the Windows taskbar, click **Start** > **Programs** > **LiveUpdate Administration Utility** > **LiveUpdate Administration Utility**.

2 Click **Retrieve Updates**.



3 In the LiveUpdate Administration Utility window, under Download Directory, type or select the download directory on your LiveUpdate server.

This is the location in which the update packages and virus definitions files will be stored once they are downloaded from Symantec. (Files are downloaded to a temporary directory that is created by the LiveUpdate Administration Utility. Once the file is downloaded, it is moved to the specified Download Directory.) The Download Directory can be any directory on your server.

4 Under Languages of Updates, select the language for downloaded packages.

5 Under Symantec Product Line, check the Symantec product lines for which you want to receive packages.

You can select individual product components to update, but you risk missing other available updates. For example, new virus definitions files for Symantec AntiVirus might require an engine update that is also available for download.

Because all installed Symantec products that use LiveUpdate now point to your intranet server, it is safer to download full product lines rather than individual products.

Uninstalling Symantec AntiVirus management components

You can uninstall all of the Symantec AntiVirus management components using Add/Remove Programs in the Control Panel on the local computer. You can also uninstall only the Symantec System Center.

Uninstalling the Symantec System Center

When you uninstall the Symantec System Center, all of its components, including snap-ins, are also uninstalled. You can uninstall the Symantec System Center using the Windows Add/Remove Programs option.

To uninstall the Symantec System Center

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec System Center**.
4. Click **Change/Remove**.
5. When the uninstallation completes, click **Close**.

Chapter 6

Installing Symantec AntiVirus servers

This chapter includes the following topics:

- Before you install
- Installing Symantec AntiVirus servers locally
- Deploying the server installation across a network connection
- About installing servers by using Microsoft SMS
- Manually installing AMS2 server
- Uninstalling Symantec AntiVirus server

Before you install

You can install the Symantec AntiVirus server program locally and across network connections, and you can install the program with and without AMS^2 server. You may also have to prepare your network connections and servers to support installation processes.

Note: As a best practice, always install a secondary server in your server group for disaster recovery purposes. The secondary server can run on operating systems that are not server operating systems, but does not support email scanning. If you do not add a secondary server and your primary management server fails, you will not be able to access the server group from the Symantec System Center.

If you do not create a secondary management server in your server group, backup the pki directory and all subdirectories. If your primary server becomes corrupt, you can recreate it if you have the backup to restore. For details, refer to the Knowledge Base articles on Symantec's Web site.

Before you install Symantec AntiVirus servers, review the following topics:

- TCP and legacy UDP communications
- Management servers and certificates

Then, review the following topics to see if they apply to your installation:

- Server installation methods
- Why AMS2 is installed with Symantec AntiVirus server
- About customizing server installations by using .msi options
- About configuring user rights with Active Directory
- Preparations for Symantec AntiVirus server installation

TCP and legacy UDP communications

This version of Symantec AntiVirus uses SSL over TCP and digital certificates to provide communication paths between the Symantec System Center, servers, and clients. The impact to Symantec AntiVirus network management administration tasks is minimal. Legacy communications occurred over UDP. If supporting legacy communications over UDP is important, you need to read and understand information about the SSL network architecture. You can also enable legacy communications in the Server Tuning Options dialog box in the Symantec System Center.

See "About migrating to the SSL communications architecture" on page 68.

Management servers and certificates

The act of making a management server a primary server creates a server group root certificate that is in the \pki\roots directory on the primary server. This certificate was created with a private key that is in the \pki\private-keys directory on the primary server.

See "Configuring a primary management server" on page 54.

The following examples show server group root certificate and private key naming conventions:

- <server-group-guid>.<counter>.servergroupca.cer
- <server-group-guid>.<counter>.servergroupca.pvk

The following examples show actual names for a certificate and private key:

- 4930435c2aa91e4abb4e6c9d527eb762.0.servergroupca.cer
- 4930435c2aa91e4abb4e6c9d527eb762.0.servergroupca.pvk

The server group root private key is used only to add new servers to a server group, so you should safely archive the key after you set up a server group with a primary server, and add at least one secondary server for disaster recovery purposes. The key is not necessary for high-volume activity, such as adding clients and authenticating users.

If you previously configured a primary server and archived the private key, you must restore this key to the private-keys directory on the primary server before you can install secondary servers in a server group. Then, archive this key again for security purposes after you install your secondary servers.

Warning: Do not lose this private key.

For more information about certificates, refer to the *Symantec AntiVirus Reference Guide* in the Docs directory on your installation CD.

Server installation methods

You can use any combination of methods that suits your network environment.

Note: Do not deploy servers in a server group until you have created a server group, installed one server in the group, and made it the primary management server for the group.

See "Configuring a primary management server" on page 54.

You can install Symantec AntiVirus servers using any of the methods that are listed in Table 6-1.

Table 6-1 Server installation methods

Method	Description	Preparation
Push	You can push a Symantec AntiVirus server installation directly from the Symantec AntiVirus CD or from the Symantec System Center. See "Deploying the server installation across a network connection" on page 115.	Install the Symantec System Center with the Symantec AntiVirus snap-in and the AV Server Rollout tool to push the server installation from the Symantec System Center.
Windows Installer (.msi) deployment	You can create and deploy an installation package using tools that are compatible with Windows Installer. Symantec AntiVirus uses Windows Installer technology for all client and server installations. Symantec AntiVirus utilizes the standard Windows Installer deployment options provided by Microsoft. To use this method, you must be familiar with creating and deploying Windows Installer programs.	■ Create a custom .msi installation package using the components and options specific to Symantec AntiVirus. See "Windows Installer (.msi) command-line reference" on page 163. ■ Determine a method for distributing and executing the package.

Why AMS^2 is installed with Symantec AntiVirus server

If you plan to use AMS^2 to generate alerts based on antivirus events, you must install AMS^2 to every primary server. While AMS^2 is required to run only on the primary server, you should install AMS^2 to all of the computers on which you install the Symantec AntiVirus server program. This lets you change primary servers without reinstalling AMS^2 on the new primary server.

If a secondary server needs to be made a primary server, no AMS^2 events will be lost. In the Symantec System Center, you can select the computer that will perform many AMS^2 actions. AMS^2 is required for some of the actions to run. Installing AMS^2 on more computers gives you flexibility in choosing the computers that can perform advanced alert actions, such as sending pages.

If you do not install AMS^2 when you install Symantec AntiVirus server, you can install it later. You must, however, install AMS^2 to the secondary server before making the secondary server the primary server.

See "Manually installing AMS2 server" on page 130.

About customizing server installations by using .msi options

The Symantec AntiVirus server installation packages are Windows Installer (.msi) files that are fully configurable and deployable using the standard Windows Installer options. You can use environment management tools that support .msi deployment, such as Active Directory or Tivoli, to install clients on your network.

See "Windows Installer (.msi) command-line reference" on page 163.

About configuring user rights with Active Directory

If you are using Active Directory to manage Windows-based computers on your network, you can create a Group Policy that provides the necessary user rights to install Symantec AntiVirus.

For more information on using Active Directory, see the Active Directory documentation provided by Microsoft.

Preparations for Symantec AntiVirus server installation

To ensure a successful Symantec AntiVirus server rollout, review the following considerations:

- About setting administrative rights to target computers
- About locating servers across routers during installation
- Creating a text file with IP addresses to import
- About verifying network access and privileges
- About deploying to a target computer without granting administrator privileges
- About installation order for Citrix Metaframe on Terminal Server
- About installing to NetWare servers
- Terminal Server protection
- Preventing user-launched virus scans

About setting administrative rights to target computers

To install Symantec AntiVirus server to a computer running supported Windows operating systems, you must have administrator rights to the computer or to the Windows domain to which the computer belongs, and log on as administrator. The Symantec AntiVirus server installation program launches a second installation program on the computer to create and start services and to modify the registry.

About locating servers across routers during installation

You can browse to find the computers on which you want to install Symantec AntiVirus server. Computers that are located across routers might be difficult to find. To verify that you can see a computer when you run the Symantec AntiVirus server installation program, try mapping a drive to the server using Windows Explorer. If you can see a computer in Windows Explorer, you should see the computer when you run the Symantec AntiVirus server installation program.

Browsing requires the use of the Windows Internet Name Service (WINS). For computers that are located in a non-WINS environment (such as a native Windows 2000 network that uses the LDAP or DNS protocol), you must create a text file with IP addresses and then import it to be able to install to those computers.

Creating a text file with IP addresses to import

You can create a text file of the IP addresses of computers that are located in a non-WINS, Windows-based environment. During installation, you can import the text file and add the listed computers to the computers on which you want to install the server program.

Note: The Import feature is designed for use with supported Windows-based operating systems only. It is not intended for use with NetWare.

To create a text file with IP addresses to import

1. In a text editor (such as Notepad), create a new text file.
2. Type the IP address of each computer that you want to import on a separate line.
   For example:
   192.168.1.1
   192.168.1.2
   192.168.1.3

You can comment out IP addresses that you do not want to import with a semicolon (;) or colon (:). For example, if you included addresses in your list for computers that are on a subnet that you know is down, you can comment them out to eliminate errors.

3 Save the file to a location that you can access when you run the server installation program.

About verifying network access and privileges

Review the following before installing the Symantec AntiVirus server program:

- Sharing must be enabled on the Windows computer on which you install Symantec AntiVirus server. The installation program uses the default shares such as c$ and admin$. When you install Windows, these shares are enabled by default. If you changed the share names or disabled sharing to the default shares, the installation program cannot complete the Symantec AntiVirus server installation.
- If you log on to a Windows domain and are put into a regular domain group without administrator rights over the local computer, you cannot install.
- Use the following command to enable server installation if you are a local administrator with a different password than the domain administrator.

  ```
  net use \\machinename\ipc$/user:username password
  ```

The rights that you need to install to server and client computers depend on the server platform and version.

About deploying to a target computer without granting administrator privileges

You can deploy an installation that does not require administrator privileges using the Microsoft Management Console. Symantec AntiVirus client and server installations are Windows Installer packages, which means that you can use elevated privilege settings to enable installation on a target computer without granting administrator privileges. For more information on enabling elevated privileges during installation for Windows Installer components, see the Microsoft Management Console documentation.

About installation order for Citrix Metaframe on Terminal Server

Symantec AntiVirus does not support drive remapping for Citrix® Metaframe®. If you plan to use Citrix Metaframe and remap your drives, complete the following tasks in the order in which they are listed:

- Install Citrix Metaframe.
- Remap the drives.
- Install Symantec AntiVirus server or client.

About installing to NetWare servers

The Symantec AntiVirus server installation program copies NLMs and other files to one or more NetWare servers that you select. To install to NetWare servers, do the following:

- Before you begin installation, log on to all of the servers to which you want to install.
  To install to the NDS or bindery, you need Admin rights.
- After you run the Symantec AntiVirus server installation program, go to the server console (or have rights to run RCONSOLE) to load the Symantec AntiVirus NLMs.
  You only need to do this manually the first time if you select the automatic startup option during setup.
  See "Manually loading the Symantec AntiVirus NLMs" on page 126.

Warning: Do not install multiple versions of Symantec AntiVirus server on a NetWare server. Either migrate or delete existing versions before installing the latest version.

About installing to a NetWare cluster

To install Symantec AntiVirus to a NetWare cluster, you install Symantec AntiVirus server on each NetWare server in the cluster following the bindery installation procedure for NetWare servers. Do not install Symantec AntiVirus to NDS.

About installing into NDS

If you browse to an NDS object to which you are not authenticated, the installation program would normally prompt you to log on. However, some versions of the Novell® client might not return a logon request, and in this case the installation program will time out or stop responding. To avoid this problem, log on to the NDS tree before running the installation program.

Protecting NetWare cluster servers and volumes

Symantec AntiVirus protects NetWare cluster servers and volumes by providing both Auto-Protect and manual scanning for each server in the cluster. Antivirus scanning of each volume in a cluster is managed by the server that has ownership of the volume. If the server with ownership of a cluster volume fails, NetWare transfers the ownership of the volume to another server in the cluster, which then automatically takes over the antivirus scanning tasks.

To protect NetWare cluster servers and volumes

- Launch Symantec AntiVirus after all volumes have been mounted and cluster services have been started in the Autoexec.ncf file.
  Launching Symantec AntiVirus once these tasks are completed ensures that all volumes are detected.

Terminal Server protection

You can install either Symantec AntiVirus client or server to Terminal Servers. Symantec AntiVirus protection works on Terminal Servers in much the same way that it works on Windows 2000/2003 file servers. Alerting is the only difference.

Note: To install the Symantec System Center on a Terminal Server, you must first stop Terminal Services. You can then restart Terminal Services after the Symantec System Center installation.

Users who are logged on to the server console receive alerts. Users who are connected through a Terminal client session do not receive alerts.

How to view Terminal Servers from the Symantec System Center console

Terminal Servers appear the same as file servers in the console from which they are managed. Both types of servers are represented with the same icon in the Symantec System Center.

Terminal Server and Terminal Services limitations

The following limitations apply to antivirus protection on Terminal Server and Terminal Services:

- Symantec AntiVirus does not protect mapped drives on computers that can be accessed by applications that are running during a session on Terminal Server.
- The file system Auto-Protect that is running on Terminal Server does not detect virus events, such as saving an infected file, that occur on local drives of Terminal Server clients.
- Symantec AntiVirus does not provide functionality to Terminal Server clients. For example, Symantec AntiVirus does not route alerts to the proper client session, or allow for the Symantec System Center to run within a session.
- Vptray.exe is the program that displays the antivirus Auto-Protect status in the system tray. Launching Vptray.exe each session is not feasible when you are scaling to a large user base due to the large footprint that is required for each session. Vptray.exe does not run if the session is remote but it does run on the Terminal Server console.
- When a user logs off of a remote Terminal session and the Auto-Protect setting to check floppy disks on computer shutdown is enabled, an unnecessary access is made to the floppy disk drive on the console. This setting is disabled by default.
- Session-specific information is not logged or included in virus alerts.

Preventing user-launched virus scans

You can prevent users from running manual scans in Terminal sessions by doing the following:

- Restrict the Windows Start menu and directories for Symantec AntiVirus to prevent users from running manual virus scans.
- Use the Application Security (AppSec) registration utility to restrict nonadministrator users to running only the programs that are included in an administrator-defined list of applications.

You can prevent users from running virus scans during Terminal sessions on a Windows 2000/2003 Terminal Services server using Application Security (AppSec). For Windows 2000/2003 Terminal Services, AppSec is included in the Windows 2000/2003 Server Resource Kit.

You must install both AppSec and the AppSec hotfix. You can find information about installing AppSec and the hotfix at:

http://www.microsoft.com/windows2000/techinfo/

To prevent users-launched virus scans

1. On the Terminal Server, on the Windows taskbar, click **Start > Programs > Windows 2000 Resource Kit > Tools**.
2. Double-click **Alphabetized List of Tools**.
3. Click **Application Security**.
4. In the Authorized Applications dialog box, in the Security group box, click **Enabled**.
   Users are denied access to any program that is not included in the Authorized Applications list, including the Symantec AntiVirus virus scanner.

Installing Symantec AntiVirus servers locally

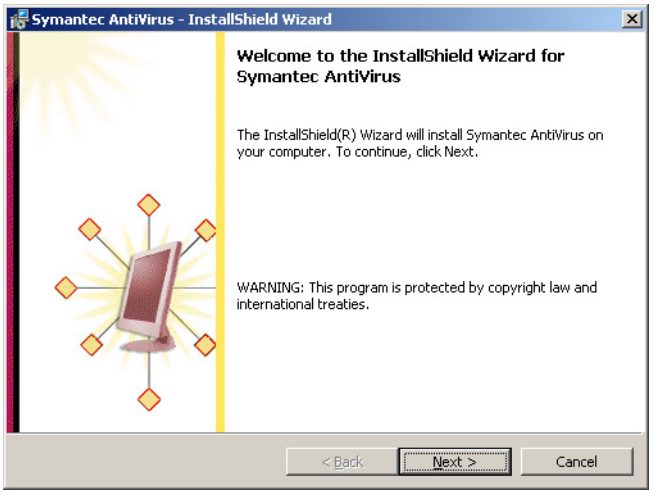
If the server computer is connected to the network, installing directly from the Symantec AntiVirus CD is the least preferred option because the CD might get damaged or lost, and only one user can install at a time.

If you make the Symantec AntiVirus CD available on a shared network drive, users must map to that drive on their workstations to ensure the successful installation of all components.

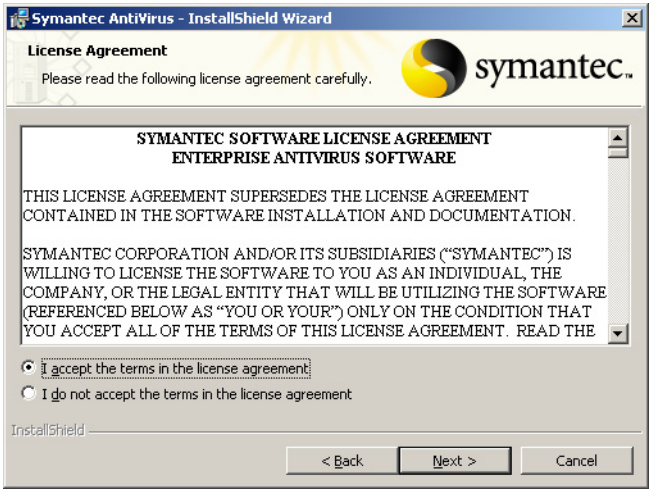
To install a Symantec AntiVirus server locally

1. Do one of the following:
   - For installation on a 32-bit computer, in the root of the CD, run Setup.exe.
   - For installation on a 64-bit computer, run Setup.exe from the \SAVWIN64 folder.
     Continue to Step 3.

2 In the Symantec AntiVirus panel, click **Install Symantec AntiVirus** > **Install Symantec AntiVirus**.


Symantec AntiVirus - InstallShield Wizard
Welcome to the InstallShield Wizard for Symantec AntiVirus
The InstallShield(R) Wizard will install Symantec AntiVirus on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

3 In the Welcome panel, click **Next**.


Symantec AntiVirus - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
symantec.
SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE
THIS LICENSE AGREEMENT SUPERSEDES THE LICENSE AGREEMENT CONTAINED IN THE SOFTWARE INSTALLATION AND DOCUMENTATION.
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

4 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.

5 In the Client Server Options panel, click **Server**, and then click **Next**.

6 In the Setup Type panel, select one of the following:

- Complete: To install all of the components that are included with the default installation.
- Custom: To exclude components from the installation or to change the installation location.

7 Click **Next**.

8 In the Select Server Group panel, do one of the following:

- Type the name of an existing Server Group, type the user name and password for that group, and then click **Next**.
- Type the name of a new server group to be created, type a user name and password, and then click **Next**. In the password confirmation dialog box, retype the password.

9 In the Install Options panel, check one of the following:

- Auto-Protect: To enable Auto-Protect
- Run LiveUpdate: To run LiveUpdate at the end of the installation

10 Click **Next**.

11 In the Ready to Install the Program panel, click **Install**.

12 If you chose to run LiveUpdate after installation, do the following:

- Follow the instructions in the LiveUpdate Wizard.
- When LiveUpdate is done, click **Finish**.

13 In the Symantec AntiVirus panel, click **Finish**.

Deploying the server installation across a network connection

You should complete each task in the order in which it is listed. The final task is required for NetWare servers only.

To push the Symantec AntiVirus server installation to computers across your network, complete the tasks that are listed in Table 6-2.

Table 6-2 Task list for installing servers across a network

Task	For more information
Start the installation.	See "Starting the server installation" on page 116.
Run the server setup program.	See "Running the server setup program" on page 117.
Select the computers to which you want to install the server program.	See "Selecting computers to which you want to install" on page 119.

Table 6-2 Task list for installing servers across a network

Task	For more information
Complete the server installation.	See "Completing the server installation" on page 122.
Review any errors.	See "Checking for errors" on page 126.
Start Symantec AntiVirus NLMs.	See "Manually loading the Symantec AntiVirus NLMs" on page 126.

Starting the server installation

You can install the Symantec AntiVirus server from the Symantec AntiVirus CD or the Symantec System Center.

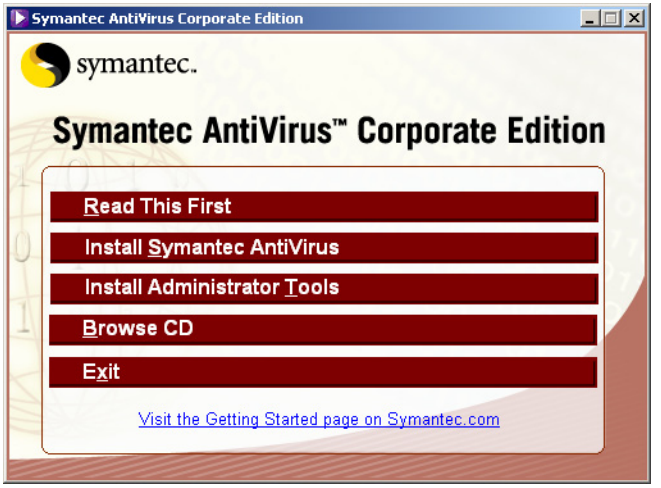
Note: When you are installing to NetWare, log on to all of the NetWare servers before you start the installation. To install to NetWare Directory Services (NDS) or bindery, you need Admin rights.

Start the server installation

You can start the server installation from the Symantec AntiVirus CD or from the Symantec System Center.

To start the installation from the CD

1 Insert the Symantec AntiVirus CD into the CD-ROM drive.



2 Click **Install Symantec AntiVirus > Deploy AntiVirus Server**.

3 Continue the installation.
See "Running the server setup program" on page 117.

To start the installation from the Symantec System Center

1 In the Symantec System Center console, in the left pane, do one of the following:
- Click **System Hierarchy**.
- Under System Hierarchy, select any object.

2 On the Tools menu, click **AV Server Rollout**.
AV Server Rollout is available only if you selected the Server Rollout component when you installed the Symantec System Center. This component is selected for installation by default.

3 Continue the installation.
See "Running the server setup program" on page 117.

Running the server setup program

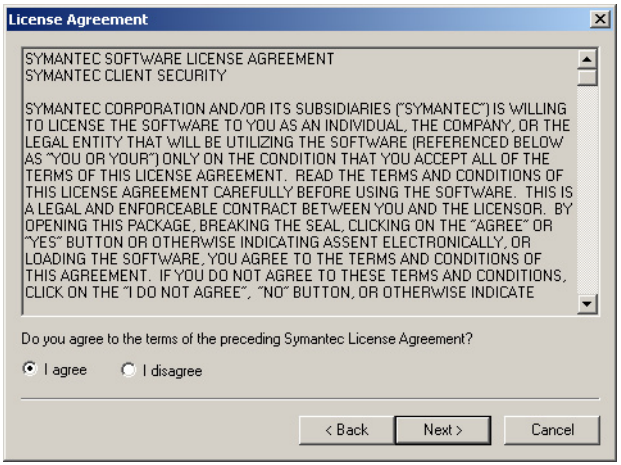
The same setup program runs no matter how you started the installation.

See "Starting the server installation" on page 116.

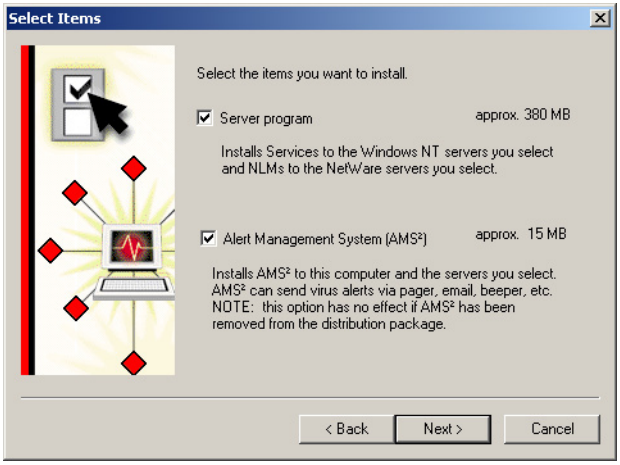
To run the server setup program

1 In the Welcome panel, do one of the following:
- To install the server to computers that have never had Symantec AntiVirus installed, click **Install**, and then click **Next**.

- To install the server to computers that have had Symantec AntiVirus previously installed, click **Update**, and then click **Next**.

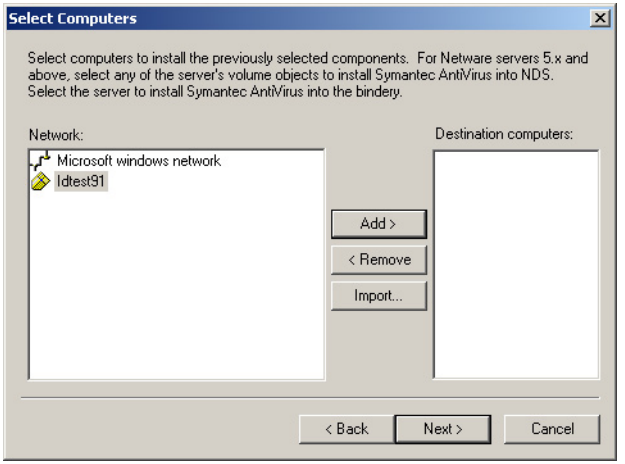

License Agreement
SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC CLIENT SECURITY
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE
Do you agree to the terms of the preceding Symantec License Agreement?
I agree
I disagree
< Back
Next >
Cancel

2 In the License Agreement panel, click **I agree**, and then click **Next**.


Select Items
Select the items you want to install.
Server program
approx. 380 MB
Installs Services to the Windows NT servers you select and NLMs to the NetWare servers you select.
Alert Management System (AMS²)
approx. 15 MB
Installs AMS² to this computer and the servers you select. AMS² can send virus alerts via pager, email, beeper, etc. NOTE: this option has no effect if AMS² has been removed from the distribution package.
< Back
Next >
Cancel

3 In the Select Items panel, ensure that Server program is checked.
If you plan to use Alert Management System^2 (AMS^2), ensure that it is checked.
See "Why AMS2 is installed with Symantec AntiVirus server" on page 106.

4 Click **Next**.


Select Computers
Select computers to install the previously selected components. For Netware servers 5.x and above, select any of the server's volume objects to install Symantec AntiVirus into NDS. Select the server to install Symantec AntiVirus into the bindery.
Network:
Microsoft windows network
ldtest91
Destination computers:
Add >
< Remove
Import...
< Back
Next >
Cancel

5 Continue the installation.
See "Selecting computers to which you want to install" on page 119.

Selecting computers to which you want to install

You can install to one or more computers. In a WINS environment, you can view the computers to which you can install. If you are installing in a non-WINS environment, you must select computers by importing a text file that contains the IP addresses of the computers to which you want to install. You can use the same import method in a WINS environment.

When you install to NDS, the computer that is performing the installation must use the Novell Client for NetWare. If you encounter problems installing to a bindery server with the Microsoft Client for NetWare, install the Novell Client for NetWare and try again.

Note: The Import feature is designed for use with Windows-based computers only. It is not intended for use with NetWare.

Select computers to which you want to install

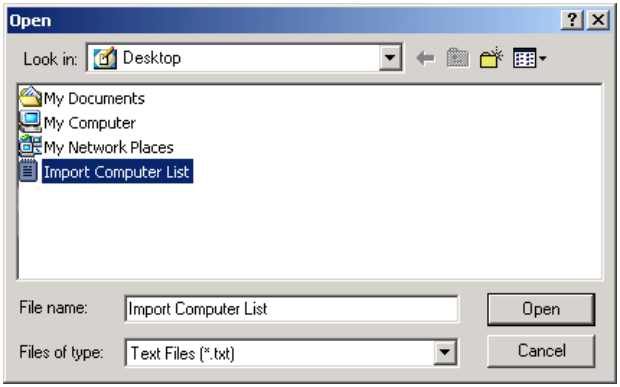
You can select Windows or NetWare computers manually or import a list of computers.

To manually select Windows computers

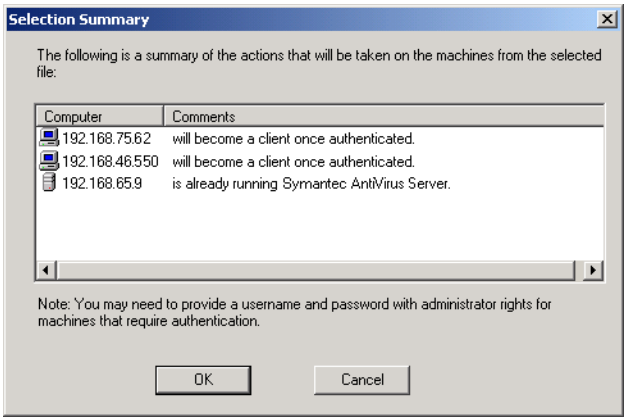
1. In the Select Computers panel, under Network, expand **Microsoft windows network**.
2. Select a server on which to install, and then click **Add**.
3. Repeat step 2 until all of the servers to which you are installing are added under Destination computers.
4. Select any NetWare computers to which you want to install.
   See "To manually select Novell NetWare computers" on page 122.
5. Continue the installation.
   See "Completing the server installation" on page 122.

To import a list of Windows 2000/XP/2003 computers

1. Prepare the list of servers to import.
   See "Creating a text file with IP addresses to import" on page 108.
2. In the Select Computers panel, click **Import**.



3 Locate and double-click the text file that contains the IP addresses to import.


Selection Summary
The following is a summary of the actions that will be taken on the machines from the selected file:
Computer
Comments
192.168.75.62
will become a client once authenticated.
192.168.46.550
will become a client once authenticated.
192.168.65.9
is already running Symantec AntiVirus Server.
Note: You may need to provide a username and password with administrator rights for machines that require authentication.
OK
Cancel

During the authentication process, you may need to provide a user name and password for computers that require authentication.

4 If you are installing to multiple computers, in the Selection Summary dialog box, click **OK**.

If you are installing to a single computer, the Selection Summary dialog box does not appear.

During the authentication process, the setup program checks for error conditions. You are prompted to view this information on an individual computer basis or to write the information to a log file for later viewing.

5 Select one of the following:

- Yes: Write to a log file.
  If you create a log file, it is located under C:\Winnt\Savcesrv.txt.
- No: Display the information on an individual computer basis.

6 Select any NetWare computers to which you want to install.

See "To manually select Novell NetWare computers" on page 122.

7 Continue the installation.

See "Completing the server installation" on page 122.

To manually select Novell NetWare computers

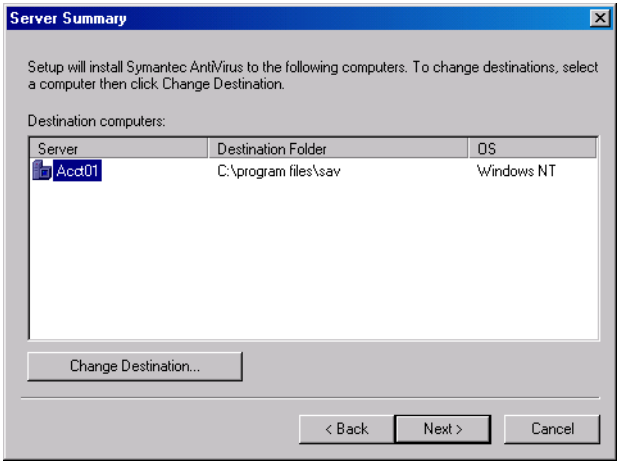
1. In the Select Computers panel, under Available Computers, double-click **NetWare Services**.
2. Do one of the following:
   - To install to a bindery server, double-click **NetWare Servers**, and then select a server (indicated by a server icon).
   - To install to NDS, double-click **Novell Directory Services**, and then select the SYS volume object in which you want to install Symantec AntiVirus.
     To locate a SYS volume object, double-click the tree object and continue expanding the organizational objects until you reach the organizational unit that contains the SYS volume object.
3. Click **Add**.
4. If you are installing to NDS, you are prompted to type a container, user name, and password.
   If you type an incorrect user name or password, the installation will continue normally. However, when you attempt to start Symantec AntiVirus on the NetWare server, you will receive an authentication error and be prompted for the correct user name and password.
5. Repeat steps 1 through 4 until the volumes for all of the servers that you are installing to are added under AntiVirus Servers.
6. Select any Windows computers to which to install.
   See "To manually select Windows computers" on page 120.
   See "To import a list of Windows 2000/XP/2003 computers" on page 120.
7. Continue the installation.
   See "Completing the server installation" on page 122.

Completing the server installation

After you have selected the computers to which you want to install, you can complete the installation. All of the computers are added to the same server group, but you can create new server groups and move servers to them in the Symantec System Center console.

To complete the server installation

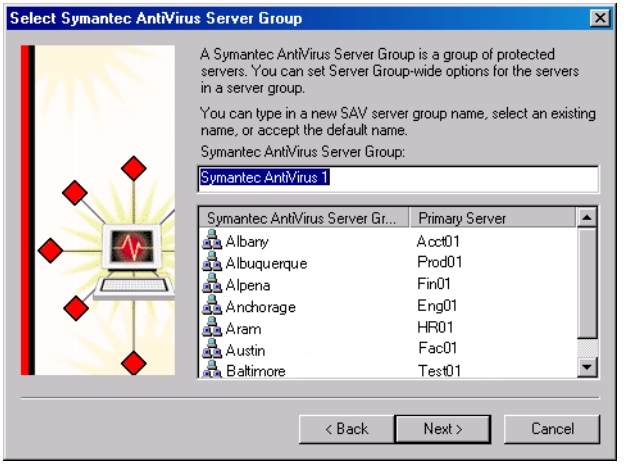
1 In the Select Computers panel, click **Finish**.



2 In the Server Summary panel, do one of the following:

- To accept the default Symantec AntiVirus installation path, click **Next**.
- To change the path, select a computer, and then click **Change Destination**. In the Change Destination dialog box, select a destination, click **OK**, and then click **Next**.

  If you are installing to a NetWare server, the new folder name is limited to eight characters.



3 In the Select Symantec AntiVirus Server Group panel, do one of the following:

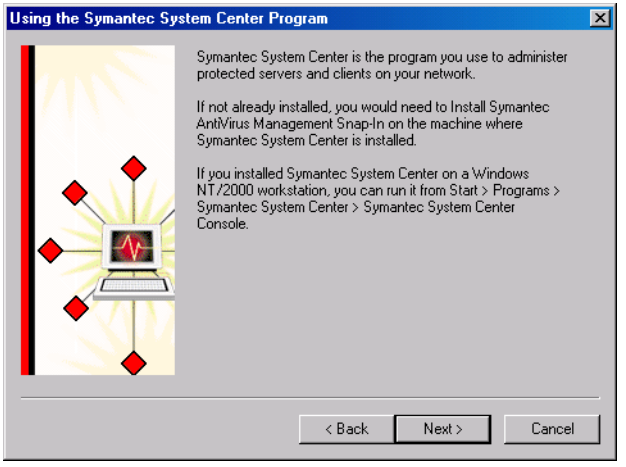
- Under Symantec AntiVirus Server Group, type a name for a new server group, and then click **Next**.
  You will be prompted to confirm the creation of the new server group and to specify a password for the server group.
- In the list, select an existing server group to join, click **Next**, and then type the server group password when you are prompted.

4 Select one of the following:

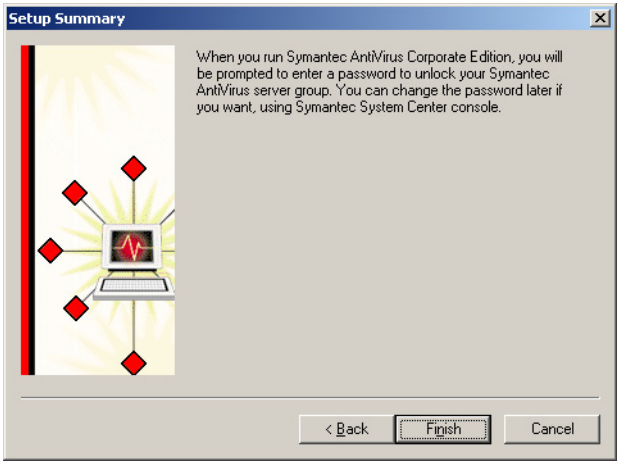
- Automatic startup: On a NetWare server, you must manually load Vpstart.nlm after you install Symantec AntiVirus server, but Vpstart.nlm will load automatically thereafter. (You must either create or join a server group during the installation process before this takes effect.)
  On a Windows-based computer, Symantec AntiVirus services (and AMS^2 services, if you installed AMS^2) start automatically every time that the computer restarts.
- Manual startup: On a NetWare server, you must manually load Vpstart.nlm after you install Symantec AntiVirus server and every time that the server restarts. Selecting this option will have no effect on Windows computers.

See "Manually loading the Symantec AntiVirus NLMs" on page 126.

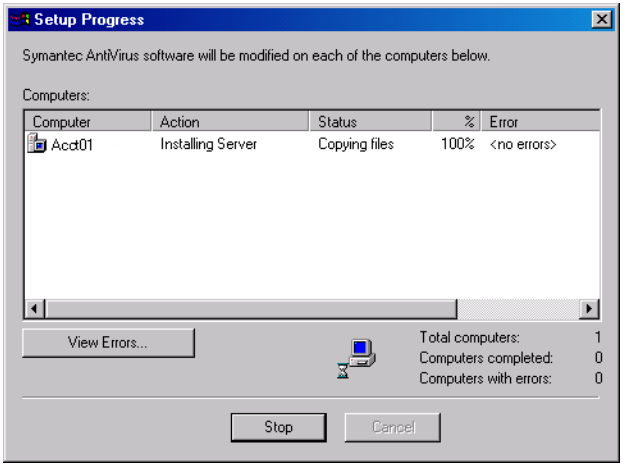
5 Click **Next**.


Using the Symantec System Center Program
Symantec System Center is the program you use to administer protected servers and clients on your network.
If not already installed, you would need to Install Symantec AntiVirus Management Snap-In on the machine where Symantec System Center is installed.
If you installed Symantec System Center on a Windows NT/2000 workstation, you can run it from Start > Programs > Symantec System Center > Symantec System Center Console.
< Back
Next >
Cancel

6 In the Using the Symantec System Center Program panel, click **Next**.


Setup Summary
When you run Symantec AntiVirus Corporate Edition, you will be prompted to enter a password to unlock your Symantec AntiVirus server group. You can change the password later if you want, using Symantec System Center console.
< Back
Finish
Cancel

7 In the Setup Summary panel, read the message that reminds you that you will need your password to unlock the server group in the Symantec System Center console, and then click **Finish**.



8 In the Setup Progress panel, view the status of the server installations.

9 Finish the installation.
See "Checking for errors" on page 126.

Checking for errors

When Symantec AntiVirus server is installed to all of the computers that you specified, you can check to see if any errors were reported.

To check for errors

1. In the Setup Progress panel, select a server, and then click **View Errors**.
2. When you are done, click **Close**.

Note: When installing to a Windows computer, you must restart the computer when the installation completes.

If you've installed to any NetWare computers, you need to load the appropriate NLMs.

See "Manually loading the Symantec AntiVirus NLMs" on page 126.

Manually loading the Symantec AntiVirus NLMs

After you install the Symantec AntiVirus server software, you must run Vpstart.nlm on each NetWare server to complete the installation. You can do this at the server console if you have rights, or by using RConsole for IP protocol networks.

Manually load the Symantec AntiVirus NLMs

After installation, you must use the /Install switch to load Vpstart.nlm for the first time. If you selected automatic startup during installation, the NLMs will load automatically the next time that the server restarts. If you selected manual startup, you must manually load Vpstart.nlm every time that you restart the server.

Note: At the NetWare console, do not add the path to the command specified. Type the command exactly as it appears. These NetWare commands are case-sensitive.

To manually load the Symantec AntiVirus NLMs for the first time

- At the server console, type the following:
  ```
  Load Sys:Sav\Vpstart.nlm /Install
  ```

  Warning: You only need to perform this procedure one time after software installation. If you use the /Install switch again, you will overwrite any current configuration settings.

To manually load the Symantec AntiVirus NLMs after NLM installation

- At the server console, type the following:
  ```
  Vpstart.nlm
  ```

Installing with NetWare Secure Console enabled

If you are using NetWare Secure Console, you can install Symantec AntiVirus while Secure Console is running. After you perform a standard Symantec AntiVirus installation, you must copy the NLM to the appropriate directory and then run the NLM on each NetWare server to complete the installation. You can do this at the server console if you have rights, or by using RConsole for IP protocol networks.

Install Symantec AntiVirus with NetWare Secure Console enabled

After installation, you must copy Vpstart.nlm from the installation directory to the Sys:\System directory and then use the /Install switch to load Vpstart.nlm for the first time. If you selected automatic startup during installation, the NLMs will load automatically the next time that the server restarts. If you selected manual startup, you must manually load Vpstart.nlm every time that you restart the server.

Note: At the NetWare console, do not add the path to the commands specified. Type each command exactly as it appears. These NetWare commands are case-sensitive.

To manually load the Symantec AntiVirus NLMs for the first time while running NetWare Secure Console

1. From the Sys:\Sav default installation directory (or the directory that was specified during installation), copy **Vpstart.nlm** to the Sys:\System directory.

2 At the server console, type the following:

```
Vpstart /install /SECURE_CONSOLE SYS:\SAV\VPSTART.NLM
```

Warning: You only need to perform this procedure one time after software installation. If you use the /Install switch again, you will overwrite any current configuration settings.

To manually load the Symantec AntiVirus NLMs after NLM installation while running NetWare Secure Console

- At the server console, type the following:

```
Vpstart.nlm
```

Installing with the server installation package

The Windows Installer (.msi) antivirus server installation package (Setup.exe) that comes with Symantec AntiVirus can be used to install directly to a supported Windows computer by executing the installation program manually or through other deployment methods, such as distributing and executing the installation using a third-party tool.

See "Installing Symantec AntiVirus using command-line parameters" on page 163.

Direct installation requires users to be logged on to the computer with administrative rights. The only exception to this is if you have enabled elevated privileges for Windows Installer packages through the Microsoft Management Console.

See "About deploying to a target computer without granting administrator privileges" on page 109.

The installation package and the supporting files must be copied to a location from which they can be run. When the package is opened, the server installation starts.

To install with the server installation package

1 On the Symantec AntiVirus CD, copy the contents of the \Rollout\AVServer folder to the location that you want.

2 Distribute the Windows Installer files using your preferred deployment method.

3 Run the installation program (Setup.exe).

About installing servers by using Microsoft SMS

Microsoft® Systems Management Server (SMS) administrators can use a package definition file (.pdf) to distribute Symantec AntiVirus management server software.

To distribute Symantec AntiVirus by using SMS, you typically complete the following tasks:

- Create a package to distribute the software.
- Generate an SMS job to distribute and install the workstation package.

In a workstation package, you define the files that comprise the software application to be distributed, and the package configuration and identification information.

To install Symantec AntiVirus management server to an existing server group, you must include the command line options SERVERGROUPNAME=, SERVERGROUPPASS=, and SERVERGROUPUSER= along with any other options.

See "Server installation properties and features" on page 167.

For an SMS deployment, the deployment package user interface has a character limit of 108 characters. Using different combinations of switches can exceed this limit and prevent the deployment.

A workaround is to change the SMS definition file (.df) to run only setup /s, and then edit the setup.ini file to include the switches that you want.

Note: If you deploy packages by using Microsoft SMS, you might need to disable the Show Status Icon On The Toolbar For All System Activity feature on the clients in the Advertised Programs Monitor. In some situations, Setup.exe might need to update a shared file that is in use by the Advertised Programs Monitor. If the file is in use, the installation will fail.

For more information on using SMS, see the Microsoft Systems Management Server documentation.

Manually installing AMS^2 server

You can manually install AMS^2 server to computers to which you've already installed Symantec AntiVirus server.

Manually install AMS^2 server

The installation methods for AMS^2 are different for Windows-based computers and NetWare servers.

Note: To avoid losing valuable information when you uninstall Symantec AntiVirus from a primary server running under NetWare, first demote the primary server from which you are uninstalling to secondary status and then promote a new server to primary status. For more information on selecting primary servers, see the *Symantec AntiVirus Administrator's Guide*.

To manually install AMS^2 server to Windows 2000/XP/2003 computers

1. Insert the Symantec AntiVirus CD into the CD-ROM drive.
2. Run the Setup.exe program, which is located in the following directory: Rollout\AVServer\Ams2\Winnt
3. Follow the on-screen instructions.

To manually install AMS^2 server to NetWare servers

1. Uninstall the Symantec AntiVirus server.
   See "Uninstalling Symantec AntiVirus server" on page 130.
2. Run the server setup program.
   See "Running the server setup program" on page 117.
3. When prompted, ensure that Alert Management System^2 (AMS^2) is checked.

Uninstalling Symantec AntiVirus server

You should uninstall Symantec AntiVirus servers and clients using the automatic uninstallation program that is provided by Symantec. If a manual uninstallation is required, see the support Knowledge Base on the Symantec Web site.

If a Symantec AntiVirus server is managing Symantec AntiVirus clients and you plan to uninstall and then reinstall the Symantec AntiVirus server software, ensure that the computer to which you reinstall has the same computer name

and IP address. If this information changes, clients will not be able to locate their parent server.

If you don't plan to replace a Symantec AntiVirus server that is managing Symantec AntiVirus clients, you should reassign any clients that are managed by the server before you uninstall the Symantec AntiVirus server software. For more information, see the *Symantec AntiVirus Administrator's Guide*.

Uninstall Symantec AntiVirus server

You can uninstall Symantec AntiVirus server from computers running supported Microsoft Windows operating systems and NetWare computers.

Note: To avoid losing valuable information when you uninstall Symantec AntiVirus from a primary server running under NetWare, first demote the primary server from which you are uninstalling to secondary status and then promote a new server to primary status. For more information on selecting primary servers, see the *Symantec AntiVirus Administrator's Guide*.

To uninstall Symantec AntiVirus server from a computer running a supported Windows operating system

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel.**
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec AntiVirus Server**.
4. Click **Remove**.

To uninstall Symantec AntiVirus server from NetWare computers

1. To switch to the Symantec AntiVirus Corporate Edition screen on the server, press **Ctrl+Esc**, and then click **Symantec AntiVirus Corporate Edition**.
2. To unload the NLMs, press **Alt+F10**.
3. At the server console, at the command prompt, type the following:

```
load Sys:\sav\Vpstart.nlm /remove
```

Chapter 7

Installing Symantec AntiVirus clients

This chapter includes the following topics:

- Before you install
- Installing Symantec AntiVirus clients locally
- Deploying the client installation across a network connection
- Installing from the client installation folder on the server
- Web-based deployment
- Installing clients by using logon scripts
- Configuring automatic client installations from NetWare servers
- About installing clients using third-party products
- Post-installation client tasks
- Configuring clients with the Grc.dat configuration file
- Uninstalling Symantec AntiVirus clients

Before you install

You can install the Symantec AntiVirus client program across network connections and locally. Before you install Symantec AntiVirus clients, review the following topics to see if they apply to your installation:

- About creating a primary management server
- About client installation methods
- About customizing client installation files by using .msi options
- About configuring user rights with Active Directory
- About Symantec AntiVirus client on a Terminal Server
- About Windows cluster server protection
- About email support
- About the client configurations file

About creating a primary management server

Before you install managed clients, you must create a primary server in the Symantec System Center for the server group that will contain the client. If you do not create a primary server before you install managed clients, you will not be able to manage your clients.

See "Configuring a primary management server" on page 54.

About client installation methods

You can use any combination of methods that suits your network environment.

You can install Symantec AntiVirus client using any of the methods that are listed in Table 7-1.

Table 7-1 Client installation methods

Method	Description	Preparation
Push	You can push the Symantec AntiVirus client installation directly from the Symantec AntiVirus CD and from the Symantec System Center. This method lets you install on computers running supported Microsoft Windows operating systems without giving users administrative rights to their computers. See "Deploying the client installation across a network connection" on page 143.	Install the Symantec System Center with the antivirus management snap-in, and use the ClientRemote Install tool to push the client installation from the Symantec System Center.
From a server	You can run Symantec AntiVirus client installation from the Symantec AntiVirus server that you want to act as a parent server. See "Installing from the client installation folder on the server" on page 147.	■ Install Symantec AntiVirus server. ■ Have users map a drive to the VPHOME\clt-inst\WIN32 share on Symantec AntiVirus server to ensure a successful installation.
Web	Users download client installation files from an internal Web server, and then run the installation. This option is available for computers that are running a supported Windows operating system. See "Web-based deployment" on page 148.	■ Ensure that the Web server meets the minimum requirements. ■ Prepare the internal Web server for deployment. ■ Copy the default client installation files to the Web server or create a custom installation, if desired.
Local	You can run the installation directly from the Symantec AntiVirus CD. This is the primary installation method supported for 64-bit computers. See "Installing Symantec AntiVirus clients locally" on page 139.	None.

Table 7-1 Client installation methods

Method	Description	Preparation
Third-party tools	You can use a variety of third-party installation tools to distribute the Windows Installer-based installation files. See "About installing clients using third-party products" on page 158.	■ See the documentation that came with your third-party installation tool for instructions on using the tool. ■ Create a custom .msi installation using the components and options specific to Symantec AntiVirus installations. See "Windows Installer (.msi) command-line reference" on page 163.

About customizing client installation files by using .msi options

The Symantec AntiVirus client installation files are Windows Installer (.msi) files that are fully configurable and deployable using the standard Windows Installer options. You can use environment management tools that support .msi deployment, such as Active Directory or Tivoli, to install clients on your network.

See "Windows Installer (.msi) command-line reference" on page 163.

About configuring user rights with Active Directory

If you are using Active Directory to manage Windows-based computers on your network, you can create a Group Policy that provides the necessary user rights to install Symantec AntiVirus.

For more information on using Active Directory, see the Active Directory documentation provided by Microsoft.

About Symantec AntiVirus client on a Terminal Server

The Symantec AntiVirus client program can be installed on a Terminal Server. The same considerations and limitations that apply to running the Symantec AntiVirus server on a Terminal Server apply to the Symantec AntiVirus client program.

About Windows cluster server protection

You can protect and manage Windows cluster servers with Symantec AntiVirus.

To protect cluster servers, complete the following tasks:

- Install the Symantec AntiVirus client to each local computer that is part of the cluster server. Do not install to the shared drives.
- Roll out Symantec AntiVirus clients using the local server names rather than the shared cluster name.

Each Symantec AntiVirus client is managed separately and provides protection in the event of a failover. You can synchronize the manageability of the clients if they are managed by the same Symantec AntiVirus server and configuration is performed at the server level.

The shared drives are protected in real time by Auto-Protect on each computer when the computer has control of the drives. When control of the shared drives is passed to another computer, Auto-Protect on that computer automatically takes over the protection.

If a manual scan of the shared drives is being performed when a failover occurs, the scan does not restart on the new computer. You must initiate a new scan.

If one Symantec AntiVirus client in the cluster is unavailable temporarily, it receives the latest virus definitions when the Symantec AntiVirus service starts and the client checks in with the parent.

Logs and alerts include the name of the local computer but they do not include the cluster server name. This helps to identify which computer had the event.

Warning: Problems might occur if Symantec AntiVirus server or client is installed to a shared drive. For example, only one client and the shared drives will be protected. Also, manageability is lost after a failover.

About email support

Symantec AntiVirus can interface with supported email client software. This provides an additional level of antivirus protection that works in conjunction with Symantec server-side email protection products. It does not replace them.

The Symantec AntiVirus client installation program automatically detects installed Microsoft Exchange/Outlook and Lotus Notes clients and selects the appropriate option for installation. If you do not want to install the extra layer of protection provided by the email support, you can deselect each component during installation.

If these email clients are not installed before installing Symantec AntiVirus, the default installation process does not install the Auto-Protect plug-in. To install the plug-ins before installing the email clients, you can select Custom when installing from the CD, or add the appropriate .msi file commands with customized installation files.

Note: If Lotus Notes is open when Symantec AntiVirus is installed, antivirus protection will not begin until Lotus Notes is restarted. Lotus Notes should be closed for five minutes after Symantec AntiVirus is installed and the Symantec AntiVirus service starts.

For users who regularly receive large attachments, you may want to disable Auto-Protect for email clients or not include the mail plug-in as part of the installation files. When Auto-Protect is enabled for email, attachments are immediately downloaded to the computer that is running the email client and scanned when the user opens the message. Over a slow connection with a large attachment, this slows mail performance.

Note: Symantec AntiVirus does not support the scanning of Exchange files or folders that are used on a Microsoft Exchange server. Scanning an Exchange directory can cause false positive virus detections, unexpected behavior on the Exchange server, or damage to the Exchange databases. If you install Symantec AntiVirus on a computer that is a Microsoft Exchange server, you should exclude the Microsoft Exchange directory structure from Auto-Protect scans.

For more information on excluding directories on email servers from Auto-Protect scans, see the *Symantec AntiVirus Reference Guide*. For additional information on using Symantec AntiVirus products with Exchange servers, see the Symantec Knowledge Base.

Symantec AntiVirus protects both incoming and outgoing email messages that use the POP3 or SMTP communications protocol. When Auto-Protect scanning for Internet email is enabled, Symantec AntiVirus scans both the body text of the email and any attachments that are included. If you do not want to install the extra layer of protection provided by Internet email support, you can deselect the Internet email scanning component during installation.

Note: If your network is configured to use non-standard ports for the POP3 or SMTP protocols, after you have installed Symantec AntiVirus you must configure the POP3 or SMTP ports that Symantec AntiVirus scans to match the ports that you are using for these protocols on your network.

For more information, see the *Symantec AntiVirus Administrator's Guide*.

About the client configurations file

If you want the client to report to a specific parent server, you must do one of the following:

- Copy the appropriate configurations file (Grc.dat) to the client after it has been installed.
  See "Configuring clients with the Grc.dat configuration file" on page 160.
- Install the client using the .msi command-line parameter that specifies the parent server.
  See "Windows Installer (.msi) command-line reference" on page 163.

Installing Symantec AntiVirus clients locally

If the client computer is connected to the network, installing directly from the Symantec AntiVirus CD is the least preferred option because the CD might get damaged or lost, and only one user can install at a time. Also, installing Symantec AntiVirus client in managed mode is more difficult because the user must specify a Symantec AntiVirus server to connect to when installing from the CD.

If users do not specify a Symantec AntiVirus server to connect to when they install from the Symantec AntiVirus CD, the Symantec AntiVirus client is installed in unmanaged mode. This means that users are responsible for getting their own virus definitions files and program updates using the Internet.

To change the client's status to managed, use one of the following methods:

- Reinstall the client from the server or use one of the other installation methods.
- Copy the configurations file (Grc.dat) from the intended parent server to the client. (This method is faster and requires fewer resources.)
  See "Configuring clients with the Grc.dat configuration file" on page 160.

If you make the Symantec AntiVirus CD available on a shared network drive, users must map to that drive on their workstations to ensure the successful installation of all components.

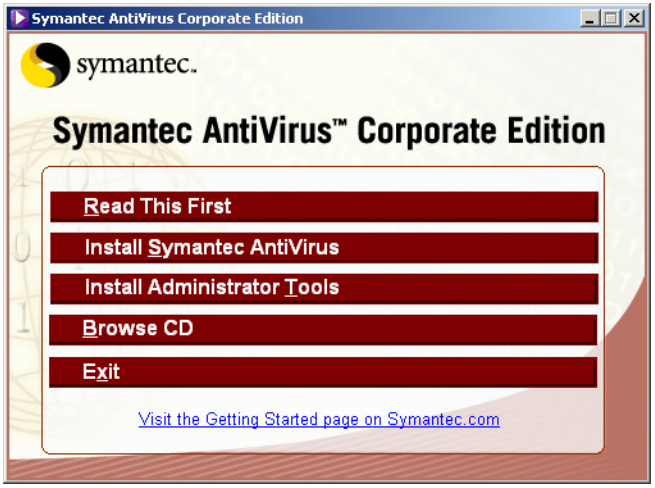
Install Symantec AntiVirus clients locally

When you install Symantec AntiVirus client, you start the installation, set up the client as either a managed or unmanaged client, and finish the installation.

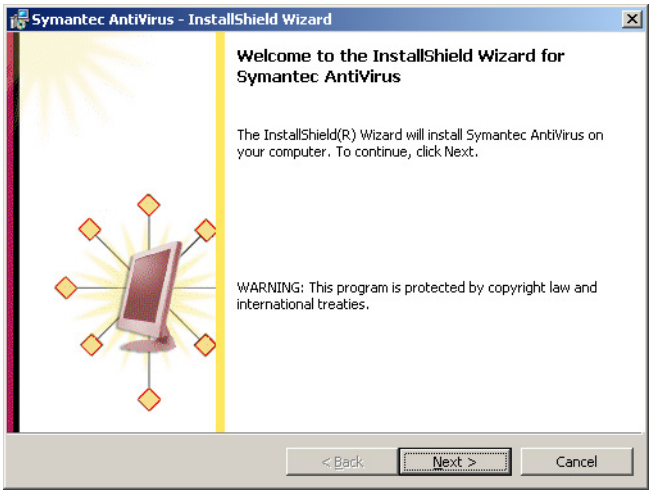
To start the installation

1. If users will run the client in managed mode, inform them of the Symantec AntiVirus server to which they will connect.
   The installation program prompts them for this information.
2. Give users access to the Symantec AntiVirus CD.
3. Do one of the following:
   - For installation on a 32-bit computer, in the root of the CD, have users run Setup.exe.
   - For installation on a 64-bit computer, run Setup.exe from the D:\SAVWIN64 folder. Follow the on-screen instructions.

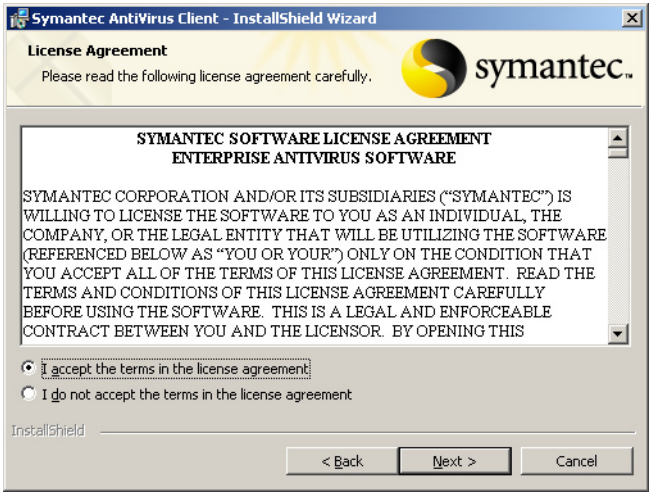
Warning: If the 32-bit version of Setup.exe is run on a 64-bit computer, the installation may fail without notification. For 64-bit installations, run Setup.exe from the \SAVWIN64 folder in the root of the CD.



4 In the Symantec AntiVirus panel, click **Install Symantec AntiVirus > Install AntiVirus Client**.


Symantec AntiVirus - InstallShield Wizard
Welcome to the InstallShield Wizard for Symantec AntiVirus
The InstallShield(R) Wizard will install Symantec AntiVirus on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

5 In the Welcome panel, click **Next**.


Symantec AntiVirus Client - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
symantec.
SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

6 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.

7 In the Client Server Options panel, click **Client**, and then click **Next**.

8 In the Setup Type panel, select one of the following:
- Complete: To install all of the components that are included with the default installation.
- Custom: To customize the installation.
  For example, in the Custom panel, you can deselect any email protection components that you do not want to install.

9 Click **Next**.

10 In the Network Setup Type panel, do one of the following:
- To have the client be managed by a parent server, click **Managed**, and then click **Next**.
  Continue with "To set up and finish a managed installation" on page 142.
- To have the client run without a parent server, click **Unmanaged**, and then click **Next**.
  Continue with "To finish an unmanaged installation" on page 142.
- If you are migrating from a previous version of Symantec AntiVirus as a managed client, the Network Setup Type panel does not appear.
  Continue with "To finish an unmanaged installation" on page 142.

To set up and finish a managed installation

1 In the Select Server panel, do one of the following:
- In the Server Name text box, type the name, and then click **Next**.
- Click **Browse**, select a server, click **OK** to confirm, and then click **Next**.
  If you don't see the server that you want, click **Find Computer** and search for the computer by name or IP address.

2 In the Ready to Install the Program panel, click **Install**.

To finish an unmanaged installation

1 In the Install Options panel, do the following:
- If you want to enable Auto-Protect, ensure that Auto-Protect is checked.
- If you want to run LiveUpdate at the end of the installation, ensure that LiveUpdate is checked.

2 Click **Next**.

3 In the Ready to Install the Program panel, click **Install**.

4 If you chose to run LiveUpdate after installation, do the following:
   - Follow the instructions in the LiveUpdate Wizard.
   - When LiveUpdate is done, click **Finish**.

5 In the Symantec AntiVirus panel, click **Finish**.

Deploying the client installation across a network connection

You can remotely install the Symantec AntiVirus client to computers running supported Microsoft Windows operating systems that are connected to the network. You can install to multiple clients at the same time without having to visit each workstation individually.

An advantage to remote installation is that users do not need to log on to their computers as administrators prior to the installation if you have administrator rights to the domain to which the client computers belong.

To push the Symantec AntiVirus client installation to computers across your network, complete the following tasks in the order in which they are listed:

- Start the Symantec AntiVirus client installation.
  See "Starting the client installation" on page 143.
- Run the Symantec AntiVirus client setup program.
  See "Running the client setup program" on page 144.

Starting the client installation

You can install the Symantec AntiVirus client using the ClientRemote Install tool.

Start the client installation

You can install the Symantec AntiVirus client from the Symantec AntiVirus CD or from the Symantec System Center.

To start the client installation from the CD

1 Insert the Symantec AntiVirus CD into your CD-ROM drive.

2 In the Symantec AntiVirus panel, click **Install Symantec AntiVirus > Deploy AntiVirus Client to 2000/XP**.

3 Continue the installation.
  See "Running the client setup program" on page 144.

To start the client installation from the Symantec System Center

1. In the Symantec System Center console, in the left pane, do one of the following:
   - Click **System Hierarchy**.
   - Under System Hierarchy, select any object.
2. On the Tools menu, click **ClientRemote Install**.
   ClientRemote Install is available only if you selected the ClientRemote Install tool when you installed the Symantec System Center. This component is selected for installation by default.
3. Continue the installation.
   See "Running the client setup program" on page 144.

Running the client setup program

The client setup program runs after you start the installation process.

See "Starting the client installation" on page 143.

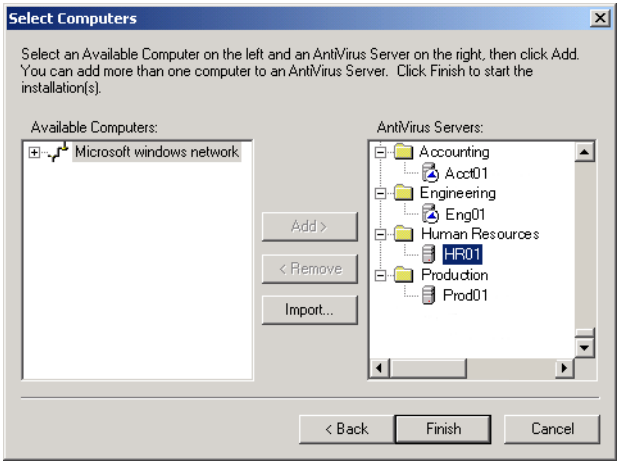
When you use the ClientRemote Install tool, in the Select Install Source Location dialog box, you can select either Default or Browse. When you select the default location, the client installation is deployed from the default location as a managed client.

When you select Browse, the Select Computers dialog box appears. Selecting your own source location implies that you have a Grc.dat among the installation files. The Grc.dat determines a client's parent server. Selecting a server to which you attach clients in the Select Computers dialog box does not determine the parent server for the client because the Grc.dat setting overwrites your selection in this dialog box. Therefore, in the Select Computers dialog box, the only important choice is the clients that you select.

To run the client setup program

1. In the Welcome panel, click **Next**.
2. In the Select Install Source Location panel, select the location from which you are deploying the client installation files.

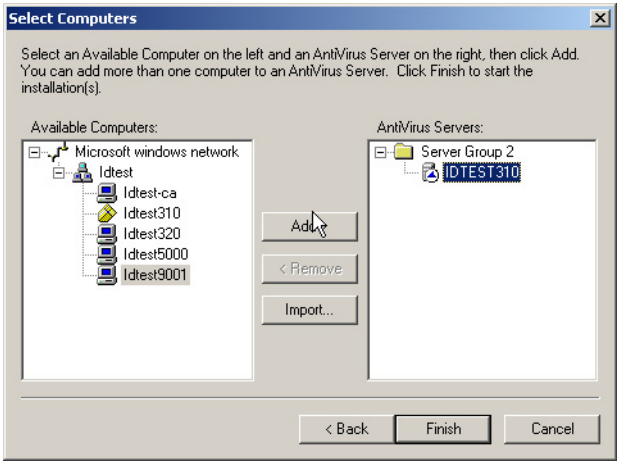
3 After you have selected the location, click **Next**.



4 In the Select Computers panel, under AntiVirus Servers, select a computer to act as the parent server.

5 Under Available Computers, expand **Microsoft windows network**, and then select a computer.

6 Click **Add**.



7 Repeat steps 5 and 6 until all of the clients that you want to manage are added.

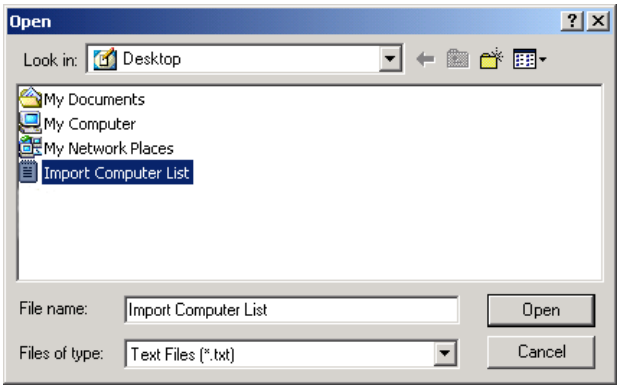
You can reinstall to computers that are already running Symantec AntiVirus. You can also import a text file to add Windows-based clients.

8 Do one of the following:

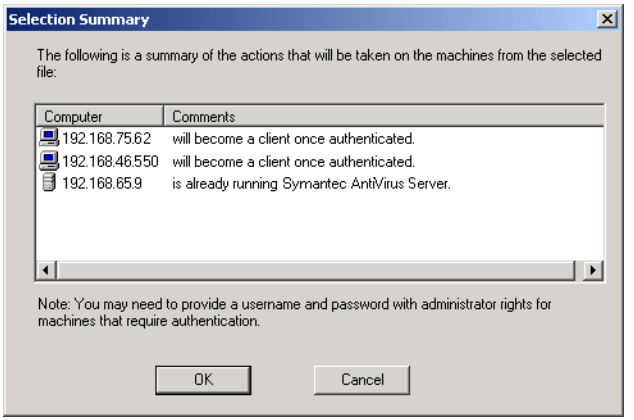
- If you created a text file that contains IP addresses to import computers that are in non-WINS environments, continue to step 9.
- If you did not create a text file that contains IP addresses to import computers in non-WINS environments, continue to step 11.

See "Creating a text file with IP addresses to import" on page 108.

9 To import the list of computers, click **Import**.



10 Locate and double-click the text file that contains the computer names.


Selection Summary
The following is a summary of the actions that will be taken on the machines from the selected file:
Computer
Comments
192.168.75.62
will become a client once authenticated.
192.168.46.550
will become a client once authenticated.
192.168.65.9
is already running Symantec AntiVirus Server.
Note: You may need to provide a username and password with administrator rights for machines that require authentication.
OK
Cancel

A summary list of computers to be added under Available Computers appears.

During the authentication process, you may need to provide a user name and password for computers that require authentication.

11 In the Selection Summary dialog box, click **OK**.
During the authentication process, Setup checks for error conditions. You are prompted to view this information interactively on an individual computer basis or to write the information to a log file for later viewing.
If you create a log file, it is located under C:\Winnt\Savcecln.txt.

12 Select one of the following:
- Yes: Display the information.
- No: Write to a log file.

13 In the Select Computers panel, click **Finish**.

14 In the Status of Remote Client Installations window, click **Done**.

Installing from the client installation folder on the server

When you install a Symantec AntiVirus server, the server setup program creates a client installation shared folder on that Symantec AntiVirus server.

On servers running supported Microsoft Windows operating systems, the default shared directory for Symantec AntiVirus server is \\Server\Vphome\Clt-inst. Everyone has read permissions.

On NetWare servers, the default shared directory is \\Server\Sys\Sav\Clt-inst. The setup program also creates a group called SymantecAntiVirusUser. If you add users to this group, they will have the rights that they need (Read and File Scan) to run the client installation program from the client disk image on the server.

When a networked user runs the client installation from the server that will manage it, the client installs in managed mode. When its associated server is selected in the Symantec System Center tree in the left pane, the client displays in the right pane. In the Symantec System Center, you can configure and manage the client.

If you want to make the Symantec AntiVirus client installation files available on a custom shared network drive, users must map to that drive on their workstations to ensure the successful installation of all components.

To install from the client installation folder on the server

1 Verify that users have rights to the client installation folder on the server.

2 Distribute the path to users and, if necessary, include drive mapping instructions to the client installation folder.
For NetWare servers, the default path is \\Server\Sys\Sav\Clt-inst.

For Windows servers, the default share path is \\Server\Vphome\Clt-inst.
The following installation folder and setup program is available in the Clt-inst folder on each server:
Clt-inst\Win32\Setup.exe

Web-based deployment

The Symantec AntiVirus client installation program is a Windows Installer-based program that can be deployed using a wide variety of deployment tools, including Web-based deployment tools, that support Windows installation files.

Deploying files through Web-based deployment requires the following steps:

- Review the Web-based deployment requirements.
- Install the Web server, if necessary.
- Set up the installation Web site.
- Customize the deployment files: Start.htm and Files.ini.
- Test the installation.
- Notify users of the download location.

The Web-based deployment tool supports the deployment of Windows Installer (.msi) files, along with any other files that the installation requires.

Web-based deployment requirements

Before you begin to implement a Web-based deployment, you should review the requirements in Table 7-2 for the Web server and the target computer.

Table 7-2 Web server and target computer requirements

Deployment on	Requirements
Web server	■ HTTP Web server. ■ Microsoft Internet Information Server (IIS) version 4.0/5.0, and Apache® HTTP Server version 1.3 or later (UNIX® and Linux® platforms are also supported).
Target computer	■ Internet Explorer 5.5 with Service Pack 2 or later. ■ Browser security must allow ActiveX® controls to be downloaded to the target computer. When the installation is complete, the security level can be restored to its original setting. ■ Computer must meet system requirements of the product to be installed. ■ User must be logged on to the computer with the rights that the product requires to be installed.

About the Web server installation

For additional information on the Web server installation, see the documentation that was supplied with the following products:

- Internet Information Server (IIS) 5.0: Installs by default during a Windows Server installation. If the IIS installation option was unchecked when Windows was installed, use the Windows installation CD to add the IIS service.
- Apache Web Server: Installs to version 2.0 or later, for Windows. (UNIX and Linux platforms are also supported.) The Apache Web Server can be downloaded from the Apache Software Foundation Web site at: http://www.apache.org

Setting up the Web server

To set up the Web server, complete the following tasks in the order in which they are listed:

- Copy the installation files to the Web server.
- Configure the Web server.

Copying the installation files to the Web server

The same procedure is used for Internet Information Server and Apache Web Server.

To copy the installation files to the Web server

1. On the Web server, create a directory called Deploy.
2. Copy the Webinst folder from the Tools folder on the Symantec AntiVirus CD to the Deploy directory.
   Alternately, if Symantec AntiVirus server is installed on the Web server, you can copy the Web Install folder to the Deploy folder.
   The default location of the Web installation directory on the server is \Clt-inst\Webinst\.

3 Copy the Grc.dat and installation files to the Deploy\Webinst\Webinst folder on the Web server from one the following locations:
   - The \\Server\Vphome\Clt-inst\Win32 shared folder on the Windows-based computer that is running the server that you want to act as the parent server
   - The \\Server\Sys\Sav\Clt-inst\Win32 shared folder on the NetWare server that is running the server that you want to act as the parent server

Finished structure

When you are finished, the folder structure on the Web server will look as follows (note that all files are case-sensitive):

- Deploy\Webinst
  - brnotsup.htm
  - default.htm
  - intro.htm
  - logo.jpg
  - oscheck.htm
  - plnotsup.htm
  - readme.htm
  - start.htm
  - webinst.cab
- Deploy\Webinst\Webinst
  - files.ini
  - The installation files (for example, Install_File.msi, Setup.exe, and so forth).

Configuring the Web server

You must configure the Web server to create a virtual directory.

Configure the Web server

You can configure Internet Information Server or Apache Web Server.

To configure Internet Information Server

1 To launch Internet Services Manager, click **Start** > **Programs** > **Administrative Tools** > **Internet Services Manager**.

2 Double-click the Web server icon to open it.

3 Right-click **Default Web Site**, and then click **New** > **Virtual Directory**.

4 To begin the Virtual Directory Creation Wizard, click **Next**.

5 In the Alias text box, type a name for the virtual directory (for example, ClientInstall), and then click **Next**.

6 Type the location of the installation folder where Deploy is located, and then click **Next**.

7 For access permissions, check **Read only**, and click **Next**, and then click **Finish**.

8 Right-click the new virtual directory, and then click **Properties**.

9 In the Properties window, on the Virtual Directory tab, change the Execute Permissions to None, and then click **OK**.

To configure Apache Web Server

1 In a text editor, open **Srm.conf**.
The Srm.conf file is installed by default under C:\Program Files\Apache Group\Apache\conf.

2 Type the following five lines at the end of the Srm.conf file:

```
DirectoryIndex default.htm
<VirtualHost 192.168.11.123>
#ServerName machinename
DocumentRoot "C:\Client\Webinst"
</VirtualHost>
```

For the VirtualHost	Replace 192.168.11.123 with the IP address of the computer on which Apache HTTP Server is installed.
For ServerName	Replace machinename with the name of the server.
For the DocumentRoot	Specify the folder in which you copied the Web installation files (for example, "C:\Client\Webinst"). Double quotation marks are required to specify the DocumentRoot. If the quotation marks are omitted, Apache services might not start.

Customizing the deployment files

Two files must be modified for the deployment. Start.htm resides in the root of the Webinst directory. Files.ini resides in the Webinst subdirectory.

Customizing Start.htm

The parameters in the Start.htm file contain information about the Web server and the locations of the files that need to be installed.

The configuration parameters in Table 7-3 are located near the bottom of the Start.htm file, inside the <object> tags.

Table 7-3 Start.htm parameters and values

Parameter	Value
ServerName	The name of the server that contains the installation source files. You can use Hostname, IP address, or NetBIOS name. The source files must reside on an HTTP Web server. For example, if your file uses the following object tag, replace ENTER_SERVER_NAME with the computer name or IP address where the installation source files are located: <param name="ServerName" value="ENTER_SERVER_NAME">
VirtualHomeDirectory	The virtual directory of the HTTP server that contains the installation source files. For example, if your file uses the following object tag, replace ENTER_VIRTUAL_HOMEDIRECTORY_NAME with the name of the Web installation folder of the virtual directory that you created (such as ClientInstall\webinst): <param name="VirtualHomeDirectory" value="ENTER_VIRTUAL_HOMEDIRECTORY_NAME">
ConfigFile	The path name to Files.ini relative to VirtualHomeDirectory, such as \Webinst\Files.ini.
ProductFolderName	The subdirectory that contains the source files to be downloaded locally. This subdirectory contains the installation files (for example, Webinst).
MinDiskSpaceInMB	The minimum hard disk space requirement. The default value is appropriate.
ProductAbbreviation	The abbreviation for the product. The default value is appropriate.

To customize Start.htm

1 In a text editor, open **Start.htm**.

2 Search for the <object> tags and type the correct values.
See Table 7-3, “Start.htm parameters and values,” on page 152.
To enable the Web installation, the ServerName and VirtualHomeDirectory parameters must be customized to match your Web server configuration.

3 Save **Start.htm**.

Customizing Files.ini

You modify Files.ini to contain the names of the files that you want to deploy.

You can provide the installation options in Table 7-4 by including the InstallOptions keyword in the [General] section.

Table 7-4 InstallOptions switches

Switch	Description
/qn	Install silently.
/qb	Install passively.
/l*v <log file>	Enable logging, where <log file> is the name of the log file that you want to generate.

Note: If you install by using Setup.exe, enclose the switches with double quotes after the /V and do not use a space after /V and before the first “. For example, `/V"/qn /l*v <logfile>"`.

See “Windows Installer commands” on page 165.

To customize Files.ini

1 In a text editor, open **Files.ini**, which is located in the Deploy\WEBINST\webinst folder on the server.

2 In the [Files] section, edit the line File1= so that it references the file that you want to deploy.
For example, after File1=, add the name of the .msi file that you want to deploy. Long file names are supported.

3 For each additional file, add a new File*n*= *filename* line, where n is a unique number and filename is the name of the file.
For example, File2=Grc.dat.

4 In the [Files] section, edit the line FileCount= so that it reflects the number of files that you are specifying.
For example, if you included File1, File2, and File3 lines in the [Files] section, FileCount=3.

5 In the [General] section, edit the line LaunchApplication= so that it references the program that you want to start after the download completes. For example, LaunchApplication=Setup.exe.

6 If you want to use additional installation options, add an InstallOptions line after the LaunchApplication line and specify the installation options that you want to include.
For example, `InstallOptions=/V"/qn /l*v <logfile>"`

7 Save **Files.ini**.
Some IIS configurations require that you rename the .ini file using a .txt extension. For more information, see the Symantec Knowledge Base.

Testing the installation

You can test the installation by going to a Web site.

To test the installation

1 Go to a Web site (for example, <your web site>/ClientInstall/Webinst), and then click **Install**.

2 If the installation fails, the following types of error messages could be displayed:
- If there is a problem with the parameters in Start.htm, an error message shows the path of the files that the Web-based installation is trying to access. Verify that the path is correct.
- If there is a problem in Files.ini (for example, a File not found error), compare the File1= value with the actual name of the installation file.
- Confirm that no other entries were changed during modification.

How to notify users of the download location

You can email instructions to your users to download the files that you want to deploy. To download the client installation program, users must have Internet Explorer 5.5 Service Pack 2 or later on their computers. The Internet Explorer security level for the local intranet must be set to Medium so that Symantec ActiveX controls can be downloaded to the client. When the installation is complete, the security level can be restored to its original setting.

Make sure that users understand the system requirements and have the administrator rights that are required for the products that they are installing. For example, to install Symantec AntiVirus client, users who are installing to Windows-based workstations must have administrator rights on their own computers and must be logged on with administrator rights.

If your installation restarts the client computers, notify your users that they should save their work and close their applications before they begin the installation.

You can include a URL in your email message that points to the client installation as follows:

- For Internet Information Server:
  http://Server_name/Virtual_home_directory/Webinst/
  where Server_name is the name of the Web-based server, Virtual_home_directory is the name of the alias that you created, and Webinst is the folder that you created on the Web server (for example, http://Server_name/Avclientinstall/Webinst/).
- For Apache Web Server:
  http://Server_name/Webinst/
  where Server_name is the name of the computer on which Apache Web Server is installed. The IP address of the server computer can be used in place of the Server_name.

Installing clients by using logon scripts

You can automate client installations in an Active Directory environment by using the logon script files that the Symantec AntiVirus server installation program copies to each Symantec AntiVirus server. The Logon directory contains the script files. For successful automation, you must copy the Symantec AntiVirus logon scripts to the Netlogon shared directory on a computer that is an Active Directory domain controller.

Note: Logon scripts perform default installations only. You cannot customize installations with logon scripts.

You associate logon scripts with specific users who authenticate to an Active Directory domain. For successful automated installation, the authenticated user must have elevated privileges. You enable these privileges by using an Active Directory console to edit the user's security profile and user group associations. Experiment with privileges and logon scripts until you find the most secure privileges that meet your security policy.

When a specific user authenticates to a domain with elevated privileges, the script calls a program to check the version number of the antivirus client that is currently available on the management server. If the antivirus client version on the server is later than the antivirus client version on the user's hard disk, or if the antivirus client is not installed on the user's hard disk, the client setup program runs.

You control how automated installation works by editing the Vp_Login.ini file, which is located in the Logon directory. The default Vp_Login.ini file contents are as follows:

```
[Installer]
Win32=\\SERVER-NAME\VPHOME\CLT-INST\WIN32\Setup.exe

[InstallOptions]
WinNT=NONE

[ClientNumber]
BuildNumber=012F03E8
```

The SERVER-NAME and BuildNumber values are automatically populated after Symantec AntiVirus server installation. The default [InstallOptions] value for WinNT=NONE specifies that no automated installation occurs. The other two [InstallOptions] WinNT values are OPTIONAL and FORCE. OPTIONAL prompts the user to install Symantec AntiVirus client software, and FORCE automatically installs Symantec AntiVirus client software without user intervention.

To install clients by using logon scripts

1. On the computer that runs Symantec AntiVirus server, in the Logon directory, open the Vp_Logion.ini file with an ASCII editor.
2. Change the [InstallOptions] value for WinNT to OPTIONAL or FORCE, and then save the file.
3. Copy and paste the following files from the Logon directory on the Symantec AntiVirus server to the Netlogon shared directory on a domain controller (the default location is C:\Winnt\Sysvol\Sysvol\<Domainname>\Scripts):
   - Vplogon.bat
   - Nbpshpop.exe

   If someone changed this shared directory, copy the files to the directory that is used as the netlogon share.
4. On the domain controller, open an Active Directory console.

5 For each user that you want to associate with the logon script, do the following:
   - Display the user's profile.
   - In the logon script box, type **Vplogon.bat**.
6 Close the Active Directory console.

Configuring automatic client installations from NetWare servers

If you have a Novell NetWare server but no Windows workstations on which to run the Symantec System Center, you can configure Symantec AntiVirus to install automatically on your Windows clients.

To configure automatic client installations from NetWare servers

1 Add users to the SymantecAntiVirusUser group using Nwadmin32 or ConsoleOne.
2 On the server console, load Vpregedt.nlm.
3 Click **(O)pen**.
4 Click **VirusProtect6**.
5 Press **Enter**.
6 Click **(O)pen** again, click **LoginOptions**, and then press **Enter**.
7 In the left pane of the window, click **(E)dit** to edit values.
8 Click **DoInstallOnWin95**, and then select one of the following:
   - OPTIONAL: Prompts the user whether to start the installation.
   - FORCE: Silently starts the installation.
   - NONE: Do not install.

   These entries are case-sensitive.
9 If you previously installed clients and need to force a new update, increment the WinNTClientVersion to a higher number.
10 Unload the Symantec AntiVirus NLM from the NetWare server.
11 Type the following command to reload the NLM:

```
Load Sys:\Sav\Vpstart
```

12 Test the client installation by logging on as a member of the SymantecAntiVirusUser group from a Novell NetWare client.

About installing clients using third-party products

You can install Symantec AntiVirus client using a variety of third-party products, including Microsoft Active Directory, Tivoli, Microsoft Systems Management Server (SMS), and Novell ZENworks®.

About installing clients with Active Directory and Tivoli

You can install Symantec AntiVirus client using the standard options that are provided by Active Directory and Tivoli for all Windows Installer-based installation files. In addition, Symantec AntiVirus provides a set of properties and features that let you customize the deployment options at the command line.

See "About customizing client installation files by using .msi options" on page 136.

A common scenario for network administrators who use .msi deployment through Active Directory is to patch existing installations. To patch a Windows Installer-based installation by using Active Directory, the primary method that is supported is to apply a patch (.msp) file to an installation package, and then redeploy the installation package to all of the computers that require the patch. Distributing .msp files individually as a means of updating clients is not supported by using Active Directory. For more information on working with patches by using Active Directory, see the Microsoft Knowledge Base.

For Active Directory and Tivoli deployment instructions, see the documentation on deploying Windows Installer (.msi) installation files that is provided with the environment that you use.

About installing clients with Microsoft SMS

Microsoft SMS administrators can use a package definition file (.pdf) to distribute Symantec AntiVirus to clients. For your convenience, a package definition file (Savce.pdf) is on the Symantec AntiVirus CD in the Tools\Bkoffice folder.

To distribute Symantec AntiVirus with SMS, you typically complete the following tasks:

- Create source directories to store each Symantec AntiVirus component that you plan to distribute.
- Create a query to identify clients that have sufficient free disk space to install the software.

- Create a workstation package to distribute the software.
- Generate an SMS job to distribute and install the workstation package on clients.

In a workstation package, you define the files that comprise the software application to be distributed, and the package configuration and identification information.

The Savce.pdf file has its package configuration and identification information already defined. You can import the file into your workstation package. The installation folder must be copied locally before you run the installation using SMS.

Note: If you deploy files by using Microsoft Systems Management Server (SMS), you might need to disable the Show Status Icon On The Toolbar For All System Activity feature on the clients in the Advertised Programs Monitor. In some situations, Setup.exe might need to update a shared file that is in use by the Advertised Programs Monitor. If the file is in use, the installation will fail.

For more information on using SMS, see the Microsoft Systems Management Server documentation.

About installing clients with Novell ZENworks

You can use the Novell ZENworks Application Launcher to distribute Symantec AntiVirus client.

After ZENworks is installed on the NetWare server and rolled out to NetWare clients through a logon script, complete the following tasks:

- From Network Administrator, locate an Organization Unit and create an Application Object that points to the location of the Symantec AntiVirus installation files on the server (for example, Sys:\Sav\Clt-inst\Win32\Setup.exe for Windows).
- Configure the Application Object. When you set options, you should do the following:
  - Associate the Application Object to an Organization Unit, group of users, or individual users.
  - When you set system requirements, select the operating system that matches the location of the Symantec AntiVirus installation files on the server.
- Set the Application Object installation style. For example, select Show Distribution Progress or Prompt User For Reboot If Needed.

After the preparation is completed, ZENworks pushes the Application Object to the client and launches the setup program when the client logs on. Nothing is required on the client side.

Post-installation client tasks

After the installation is complete, you may want to perform the following tasks:

- Configure clients using the configurations file.
  See "Configuring clients with the Grc.dat configuration file" on page 160.

Configuring clients with the Grc.dat configuration file

You can use the Grc.dat configurations file to configure clients when you do any of the following:

- Convert an unmanaged Symantec AntiVirus client into a managed client.
- Change the parent server of a managed client without having to uninstall and reinstall the client, especially if the parent server has crashed.

To do the above, you also have to copy the server group root certificate to the \pki\roots directory from the management server that will act as the parent of the client.

To assign the client to a parent server, complete the following tasks in the order in which they are listed:

- Obtain the configurations file.
  See "Copying the configuration files from a management server" on page 160.
- Copy the configurations file to the client.
  See "Pasting the configuration files on the client" on page 161.

Copying the configuration files from a management server

The configuration file Grc.dat contains the name of the server that you want to act as the parent server. The server group root certificate file xxx.x.servergroupca.cer contains the server group root certificate for the server group. If you copy the files from the server that you want to act as the parent server and place them on the client, you will distribute all of the client settings for that server and establish communications.

To copy the configuration files from a management server

1. Open Network Neighborhood or My Network Places.
2. Locate and double-click the computer that you want to act as the parent server.
   Symantec AntiVirus server must be installed on the computer that you select.
3. Open the VPHOME\Clt-inst\Win32 folder.
4. Copy Grc.dat to the desired location.
5. Open the pki\roots folder.
6. Copy xxx.x.servergroupca.cer to the desired location.

Pasting the configuration files on the client

You paste the configuration files in separate directories on the client. You can either copy the files manually from transportable media, network share, or email attachment, or you can use the Microsoft Installer options that are available to create and roll out an installation that contains the configuration files.

See "Windows Installer (.msi) command-line reference" on page 163.

To paste the configuration files to the client

1. Copy the Grc.dat file from the desired location.
2. Paste the Grc.dat file in the following directory on the client:
   <volume>:\Documents and Settings\All Users\
   Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5
3. Copy the xxx.x.servergroupca.cer file from the desired location.
4. Paste the xxx.x.servergroupca.cer in the following directory on the client, which appears in the directory that contains the Symantec AntiVirus files:
   \pki\roots
5. Restart the client.
   The Grc.dat configuration file disappears after you restart the client.

Uninstalling Symantec AntiVirus clients

You should uninstall Symantec AntiVirus clients using the uninstallation program that is provided by Symantec. You must uninstall Symantec AntiVirus client from the local computer. If a manual uninstallation is required, see the support Knowledge Base on the Symantec Web site.

You can uninstall Symantec AntiVirus client from Windows computers. If the clients are managed, you need to supply a password that you configure in the Symantec System Center as a Client Administrator Only Option. By default, the password is `symantec`.

Note: During the uninstallation, Windows might indicate that it is installing software. This is a general Microsoft message that can be ignored.

Before you uninstall the antivirus client, ensure that its user interface is closed. Attempting to uninstall while the main user interface runs might produce inconsistent results.

To uninstall the client

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec AntiVirus Client**.
4. Click **Remove**.
5. (Optional) If the client is managed, in the Password dialog box, type the uninstallation password, and then click **OK**.

Note: You must restart the computer before you reinstall the client.

Appendix A

Windows Installer (.msi) command-line reference

This chapter includes the following topics:

- Installing Symantec AntiVirus using command-line parameters
- Windows Installer commands
- Server installation properties and features
- Client installation properties and features
- Using the log file to check for errors
- Command-line examples

Installing Symantec AntiVirus using command-line parameters

The Symantec AntiVirus client installation programs utilize Windows Installer (.msi) packages for installation and deployment. If you are using the command line to install or deploy an installation package, you can use the standard Windows Installer switches and Symantec-specific parameters to customize the installation.

To use this Windows Installer, elevated privileges are required. If you attempt the installation without elevated privileges, the installation may fail without notice.

For the most up-to-date list of Symantec installation commands and parameters, see the Symantec Knowledge Base. For more information on using the standard Windows Installer commands, see the documentation provided by Microsoft.

Note: The Microsoft Installer advertise function is unsupported.

Default Symantec AntiVirus server installation

The default Symantec AntiVirus server installation package includes the following installation components:

- Symantec AntiVirus server base files (including the user interface) are installed.
- Symantec AntiVirus Help files are installed.
- LiveUpdate is installed and updated virus definitions files are downloaded from the Symantec Web site (if the server is connected to the Internet).

The default Symantec AntiVirus server installation package includes the following installation settings:

- Computer restart is required.
- File System Auto-Protect is enabled after the computer is restarted.

Default Symantec AntiVirus client installation

The default Symantec AntiVirus client installation package includes the following installation components:

- Symantec AntiVirus client base files (including the user interface) are installed.
- Symantec AntiVirus Help files are installed.
- Auto-Protect Email snap-ins (including Microsoft Exchange, Lotus Notes, and Internet Email) are installed and enabled if the corresponding Microsoft Exchange, Outlook, or Lotus Notes clients are detected. The Internet Email snap-in is installed by default.
- Symantec Quarantine client files are installed.
- LiveUpdate is installed and updated virus definitions files are downloaded from the Symantec Web site (if the client is connected to the Internet).

The default Symantec AntiVirus client installation package includes the following installation settings:

- The client is installed as an unmanaged client.
- Computer restart is not required.
- File System Auto-Protect is enabled after the computer is restarted.

If you want to distribute a customized Grc.dat file as part of a Symantec AntiVirus Windows Installer-based (.msi) installation package, drop the Grc.dat file in the same directory as the installation files that the installation package uses or distributes. The installation program detects the Grc.dat file, and then uses the settings that it contains.

Windows Installer commands

The Symantec AntiVirus installation packages use the standard Windows Installer commands as well as a set of extensions for command-line installation and deployment. See the Windows Installer documentation for further information on the usage of standard Windows Installer commands.

Table A-1 describes the basic set of commands that are used for Symantec AntiVirus client and server installations.

Table A-1 Commands

Command or property	Description
Symantec AntiVirus.msi	Symantec AntiVirus .msi installation file for both servers and clients. If any .msi file contains spaces, enclose the file name in quotations when used with /i and /x. Required
Msiexec	Windows Installer executable. Required
/i <“msi file name”>	Install the specified .msi file. If the file name contains spaces, enclose the file name in quotations. If the .msi file is not in the same directory from which you execute Msiexec, specify the path name. If the path name contains spaces, enclose the path name in quotations. For example, msiexec.exe /i “C:<path to> Symantec AntiVirus.msi” Required
/qn	Install silently. **Note:** Silent installation of the Symantec System Center is not supported. Optional

Table A-1 Commands

Command or property	Description
/x <“msi file name”>	Uninstall the specified components. Optional
/qb	Install with a basic user interface that shows installation progress. Optional
/l*v <log filename>	Create a verbose log file, where <log filename> is the name of the log file you want to create. Optional
INSTALLDIR=<path>	Designate a custom path on the target computer where <path> is the specified target directory. If the path includes spaces, use quotation marks. **Note:** The default directory is “C:\Program Files\Symantec AntiVirus.” Optional
REBOOT=<value>	Suppress a computer restart after installation, where <value> is a valid argument. The valid arguments include the following: ■ Force: Requires that the computer is restarted. ■ Suppress: Prevents most restarts. ■ ReallySuppress: Prevents all restarts as part of the installation process. Optional
ADDLOCAL= <feature>	Select custom features to be installed, where <feature> is a specified component or list of components. If this property is not used, all applicable features are installed by default, and AutoProtect email clients are installed only for detected email programs. See “Server installation properties and features” on page 167. See “Client installation properties and features” on page 169. To add all appropriate features for either server or client installations, use the ALL command as in ADDLOCAL=ALL. For example, on the client, this command installs all email Auto-Protect components. **Note:** When specifying a new feature to be installed, you must include the names of the features that are already installed on the target computer that you want to keep. If you do not specify the features that you want to keep, Windows Installer will remove them. Specifying existing features will not overwrite the installed features. To uninstall an existing feature, use the REMOVE command. Optional

Table A-1 Commands

Command or property	Description
REMOVE=<feature>	Uninstall the previously installed program or a specific feature from the installed program, where <feature> is one of the following: ■ <feature>: Uninstalls the feature or list of features from the target computer. ■ ALL: Uninstalls the program and all of the installed features. All is the default if a feature is not specified. Optional

Server installation properties and features

You can customize how Windows Installer server installation packages are installed by using properties and features.

Symantec AntiVirus server properties

Table A-2 describes the properties that are configurable for the Symantec AntiVirus server installation.

Table A-2 Symantec AntiVirus server properties list

Property	Description
INSTALLSERVER=1	Specifies that the installation is a server installation. A value of 0 (the default) indicates a client installation. Required
SERVERGROUPNAME=<server group name>	Specifies the name of a new or existing server group that the target will join. If the server group is new, the installation installs and configures the server as the group's primary management server, and the default logon user name is Admin. Required
SERVERGROUPUSERNAME=<username>	Specifies the name of a new or existing user name used to logon to the server group that the target server will join. The default is admin. Required
SERVERGROUPPASS=<password>	Specifies the name of a new or existing password of the server group that the target server will join. The default is symantec. Required

Table A-2 Symantec AntiVirus server properties list

Property	Description
SERVERPARENT=<parent server name>	For secondary server installations, specifies the name of the parent server. When you perform a deployment by using the Deploy Server user interface or the Symantec System Center, this property is not required. May be required
ENABLEAUTOPROTECT=<val>	Determines whether File System Auto-Protect is enabled after the installation is complete, where <val> is one of the following values: ■ 1: Enables Auto-Protect after installation (default). ■ 0: Disables Auto-Protect after installation. Optional
RUNLIVEUPDATE=<val>	Determines whether LiveUpdate is enabled as part of the installation, where <val> is one of the following: ■ 1: Enables LiveUpdate after installation (default). ■ 0: Disables LiveUpdate after installation. **Note:** LiveUpdate is a required component of the Symantec AntiVirus installation. Optional
SYMPROTECTDISABLED=<val>	Determines whether SymProtect is enabled as part of the installation, where <val> is one of the following: ■ 1: Disables SymProtect after installation. ■ 0: Enables SymProtect after installation. (default). Optional

Symantec AntiVirus server features

These features are used by the Windows Installer ADDLOCAL command to specify the features that are installed.

Table A-3 describes the features that are configurable for the Symantec AntiVirus server installation.

Table A-3 Symantec AntiVirus server features

Feature	Description
SAVMain	Specifies the basic Symantec AntiVirus server files. This feature is required.
SAVUI	Makes the user interface available to the target computer. This feature is optional.
SAVHelp	Include Symantec AntiVirus Help files. This feature is optional.

Client installation properties and features

You can customize how Windows Installer client installation packages are installed by using properties and features.

Symantec AntiVirus client properties

Table A-4 describes the properties that are configurable for the Symantec AntiVirus client installation.

Table A-4 Symantec AntiVirus client properties

Property	Description
INSTALLSERVER=0	Specifies that the installation to be used is the client installation. 0 is the default. A value of 1 indicates a server installation. Optional
NETWORKTYPE=<val>	Describes the management state of the client computer when installation is complete, where <val> is one of the following: ■ 1: Managed ■ 2: Unmanaged (default) Optional
SERVERNAME=<parent server name>	Specifies the name of the existing parent server that will manage the target computer. Required if NETWORKTYPE=1

Table A-4 Symantec AntiVirus client properties

Property	Description
ENABLEAUTOPROTECT=<val>	Determines whether File System Auto-Protect is enabled after the installation is complete, where <val> is one of the following values: ■ 1: Enables Auto-Protect after installation (default). ■ 0: Disables Auto-Protect after installation. Optional
SYMPROTECTDISABLED=<val>	Determines whether SymProtect is enabled as part of the installation, where <val> is one of the following: ■ 1: Disables SymProtect after installation. ■ 0: Enables SymProtect after installation. (default). Optional
RUNLIVEUPDATE=<val>	Determines whether LiveUpdate is enabled as part of the installation, where <val> is one of the following: ■ 1: Enables LiveUpdate after installation (default). ■ 0: Disables LiveUpdate after installation. **Note:** LiveUpdate is a required component of the Symantec AntiVirus installation. Optional

Windows Security Center features

These properties apply to unmanaged clients only. The Symantec System Center controls these properties for managed clients.

Table A-5 describes the properties that are configurable to control interaction between users and Windows Security Center (WSC) running on Windows XP with Service Pack 2.

Table A-5 Windows Security Center properties

Property	Description
WSCCONTROL=<val>	Controls WSC where <val> is one of the following: ■ 0: Do not control (default). ■ 1: Disable once, the first time it is detected. ■ 2: Disable always. ■ 3: Restore if disabled.

Table A-5 Windows Security Center properties

Property	Description
WSCAVALERT=<val>	Configures antivirus alerts for WSC where <val> is one of the following: ■ 0: Enable. ■ 1: Disable (default). ■ 2: Do not control.
WSCFWALERT=<val>	Configures firewall alerts for WSC where <val> is one of the following: ■ 0: Enable. ■ 1: Disable (default). ■ 2: Do not control.
WSCAVUPTODATE=<val>	Configures WSC out-of-date time for antivirus definitions where <val> is one of the following: 1—90: Number of days (default is 30).

Symantec AntiVirus features

There are many Symantec AntiVirus features that can be installed using a customized Windows Installer package. These features are used by the Windows Installer ADDLOCAL property to specify the features that are installed.

See "Command-line examples" on page 173.

Symantec AntiVirus client features

Table A-6 describes the features that are configurable for the Symantec AntiVirus client installation.

Table A-6 Symantec AntiVirus client features

Feature	Description
SAVMain	Specifies the basic Symantec AntiVirus client files. This feature is required.
SAVUI	Makes the user interface available to the target computer. This feature is optional.
SAVHelp	Include Symantec AntiVirus Help files. This feature is optional.
OutlookSnapin	Include the Microsoft Exchange Auto-Protect email component. This feature is optional.

Table A-6 Symantec AntiVirus client features

Feature	Description
NotesSnapin	Include the Lotus Notes Auto-Protect email component. This feature is optional.
Pop3Smtp	Include the Internet Email Auto-Protect component. This feature is optional.
QClient	Include the Symantec Quarantine client. This feature is optional.

Using the log file to check for errors

The Windows Installer creates a log file that can be used to verify whether or not an installation was successful, list the components that were successfully installed, and provide a variety of further details related to the installation package. The log file can be used as an effective tool to troubleshoot an installation package that fails.

If the installation is successful, the log file includes a success entry near the end. If the installation is not successful, an entry is created that indicates that the installation failed.

The log file(sav_inst.log) that is created by the default installation package is added to the \temp directory associated with the user that is running (or deploying) the installation package.

Note: Each time the installation package is executed, the log file is overwritten. Appending an existing log file is not supported.

Identifying the point of failure of an installation

You can use the log file to help identify the component or action that caused an installation to fail.

To identify the point of failure of an installation

1. In a text editor, open the log file that was generated by the installation.
2. Search for the following:

   `VALUE 3`

   The action that occurred before the line that contains this entry is most likely the action that caused the failure. The lines that appear after this entry are installation components that have been rolled back because the installation was unsuccessful.

Command-line examples

Table A-7 includes commonly used command-line examples.

Table A-7 Command-line examples

Task	Command line
Silently install an unmanaged Symantec AntiVirus client with default settings to c:\SFN.	msiexec /i "Symantec AntiVirus.msi" INSTALLDIR=C:\SAV /qn
Silently install a managed Symantec AntiVirus client that is managed by the SR1 server (having the password my$Pass) with all of the default features except QClient. Do not restart the computer and run LiveUpdate after installation, and do not enable Auto-Protect when the computer is (ultimately) restarted.	msiexec /i "Symantec AntiVirus.msi" ADDLOCAL=SAVMain,SAVUI, OutlookSnapin,NotesSnapin, Pop3Smtp NETWORKTYPE=2 SERVERNAME= SR1 SERVERGROUPPASS=”my$Pass” ENABLEAUTOPROTECT=0 RUNLIVEUPDATE=1 REBOOT=ReallySuppress /qn
Silently install a managed Symantec AntiVirus client to the default path that is managed by the SR1 server (having the password my$Pass) with no Symantec AntiVirus Help and no Lotus Notes Snap-in. Do not run LiveUpdate, and do not restart the computer automatically.	msiexec/i "Symantec AntiVirus.msi" ADDLOCAL=SAVMain,SAVUI, OutlookSnapin,Pop3Smtp,QClient NETWORKTYPE=1 SERVERNAME= SR1 SERVERGROUPPASS=”my$Pass” ENABLEAUTOPROTECT=1 RUNLIVEUPDATE=0 REBOOT=ReallySuppress /qn

Index

Symbols

.msi, installing using command-line parameters 163

A

Active Directory and user rights 34
Alert Management System. *See* AMS
alias 155
AMS, installing with Symantec AntiVirus server 106
AMS^2
- about the console 23
- and server installation 106
- manually installing 130

antivirus, testing detection 63
antivirus clients
- configuration files 139
- copying the configurations file to 161
- installation
  - locally 139
  - managed clients 142
  - running setup 144
  - starting 143
  - using logon scripts 155

Apache Web Server, configuring 151
AppSec 112
architecture
- planning 30
- server groups 31

automatic startup
- NLMs 110
- services 124
- Vpstart.nlm 124

Auto-Protect, testing 64
AV Server Rollout tool
- about 24
- installing with the Symantec System Center 45

C

Central Quarantine
- about 22, 36
- attaching a management server 98
- configuring servers and clients to use 98
- installing 91

Citrix Metaframe 110
ClientRemote Install tool management component 24
clients
- configuring by using the configurations file 160
- converting unmanaged to managed 160
- installation
  - about 135
  - automatic from NetWare servers 157
  - post-installation tasks 160
  - to clients 33, 108
- rolling out by using third-party products 158

cluster servers, protecting 137
communication ports 40
computers, selecting for installation 119
configuration
- Auto-Protect scanning 59
- primary server 54
- scheduled scans 58
- server group 54

configurations file
- configuring clients with 160
- copying to the antivirus client 161
- obtaining 160

conversion, unmanaged to managed clients 160

D

deployment
- antivirus clients across a network connection 143
- by using Web-based installation files 148
- customizing files 152
- over the Web 148
- requirements for Web-based 148

deployment *(continued)*
servers across a network connection 115
testing Web-based installations 154
to a target computer without granting administrator privileges 109
distribution with SMS Package Definition Files 158
download location, notifying users of 154

E

errors, server installation 126

F

Files.ini 153

G

Grc.dat. *See* configurations file

I

installation
.msi client features 171
.msi client properties 169
.msi command-line examples 173
.msi server features 168
.msi server properties 167
.msi Windows Security Center features 170
AMS^2, manual 130
antivirus clients 144
by using .msi commands 163
by using log files to identify failure points 173
Central Quarantine 91
checking for errors on servers 126
completing for servers 122
default client footprint 164
default server footprint 164
first time 43
first time installation sequence 44
from the client installation package on the server 147
how to create a text file with IP addresses to import 108
installation files from the CD 142
installing clients from the CD 62
installing clients from the Symantec System Center 60
into NDS 111
LiveUpdate Administration Utility 99
locating servers during 108
installation *(continued)*
management server from the Symantec System Center 50
Novell ZENworks Application Launcher 159
order for Citrix Mainframe on Terminal Server 110
planning 29
preparing 90
requirements 34
running the server setup program 117
selecting computers 119
server methods 103
starting server 116
Symantec System Center 45, 79
Terminal Services and the Symantec System Center 90
Web server 149
why AMS^2 is installed with the server 106
Windows Installer commands 165
with logon scripts 155
IP addresses, creating a text file for installation 108

L

LiveUpdate, about 22
LiveUpdate Administration Utility, installing 99
logon scripts, installing with 155

M

manual startup
NLMs 126
Vpstart.nlm 124
Microsoft Systems Management Server (SMS), rolling out Package Definition Files 129, 158
migration
clients 85
clients by using the CD 86
clients by using the Symantec System Center 86
how it works 70
legacy servers 69
LiveUpdate server 87
migrating the first management servers 81
NetWare 83
ordering 71
overview 67
servers 80
steps to take 71
supported and unsupported paths 72

migration *(continued)*
to the SSL communications architecture 68
unlocking the migrated server group 79

N

NetWare
about VPStart commands 84
cluster installation 110
cluster server and volume protection 111
required rights to install to servers 110
NetWare Secure Console installation 127
network 115
deploying clients across 143
traffic, client 111
traffic planning for communications 35
NLMs
automatic startup for 110
manually loading 126
Novell ZENworks, Application Launcher 159

O

operating system requirements 36

P

port communications 40
primary server, configuring 54
protocols, required 35

R

remote installation
in domains and workgroups 40
permitting on Windows XP computers 40
TCP port 139 35
required protocols 35
requirements
operating system 36
protocols 35
RAM, storage, and application 37
system time 34
rights
to install to NetWare servers 110
to install to target computers 33, 108

S

scans
preventing 112
scans *(continued)*
rescanning and submitting files to Symantec Security Response 25
scheduled scans, configuring 58
server group private key
promoting secondary server to primary server 69
securing 68
server group root certificate
copying to the Symantec System Console computer 68
naming convention 56
server group root certificate private key
naming convention 56
protecting 56
server installation
completing 122
deploying 115
enabling sharing 109
methods 103
rights 110
setup program 117
starting 116
verifying network access 109
servers, protecting cluster servers 137
setup program for servers 117
Start.htm 153
Symantec AntiVirus, Terminal Server protection 111
Symantec AntiVirus snap-in, installing with the Symantec System Center 45
Symantec Client Firewall snap-in, installing with the Symantec System Center 45
Symantec Security Response 25
Symantec System Center
about 22, 23, 36
installing 45
installing clients from 60
installing on server operating systems 44
server tuning options 33
upgrade scenarios 74
upgrading 76
system requirements
about 34
protocols 35
system time values
requirements 34
specifying in the Symantec System Center 69
synchronizing 69

T

Terminal Server 111
    installation order 110
    limitations 112
    viewing from the console 111
third-party products, using for rollout 158
Threat Tracer, testing 65

U

uninstallation
    antivirus clients 162
    management components 102
    Symantec AntiVirus servers 130
    Symantec System Center 102
upgrade
    Symantec System Center 76
    Symantec System Center scenarios 74

V

VDTM, updating server groups 57

W

Web server
    configuring 150
    copying installation files to 149
    installing 149
    setting up installation 149
Web-based deployment
    about 148
    deploying installation files by using 148
    requirements for 148
    testing installation 154
Windows Installer commands 163, 165
Windows Server 2003 36
Windows XP 40
Windows XP firewalls
    disabling 39
    using 40
Wizard, LiveUpdate 115, 143